

郑州教育管理公共数据安全防护服务等项目

招 标 文 件

招标编号：郑财招标采购-2018-48



河南招标采购服务有限公司

HENAN TENDER-PURCHASE SERVICE CO., LTD.

总目录

第一卷

第一章 招标邀请.....	3
第二章 投标人须知.....	5
第三章 合同基本格式.....	15
第四章 投标文件相关格式.....	18

第二卷

第五章 招标项目资料表.....	38
第六章 合同条款资料表.....	42
第七章 招标项目需求及技术规格要求.....	43
附件 评标标准和评标方法.....	64

第一卷

第一章 招 标 邀 请

日 期：2018 年 04 月 13 日

招标编号：郑财招标采购-2018-48

河南招标采购服务有限公司受郑州市教育局电化教育馆的委托，就郑州教育管理公共数据安全防护服务等项目进行公开招标，现欢迎符合条件的潜在投标人提供密封投标。

一、项目基本情况：

序号	货物名称	单位	数量	完工期	交货地点
1	教育应用安全态势感知平台及应急支撑	批	1	合同生效后 60 日内完成设备安装、调试、运行。	郑州市教育局电化教育馆
2	郑州教育管理公共服务数据安全防护	批	1		
3	郑州教育数据中心重要信息系统安全服务	批	1	合同生效后 60 日内完成系统评测、定级等。	
4	郑州市市直学校网站安全监测项目	套	1	合同生效后 60 日内完成系统安装、调试、运行。	

共分为一个包，采购预算为 516.67 万元，投标报价超出采购预算的为无效投标。

二、投标人资格条件：

1. 具备政府采购法第二十二条规定的条件：

- 1.1 具有独立承担民事责任的能力；
- 1.2 具有良好的商业信誉和健全的财务会计制度；
- 1.3 具有履行合同所必需的设备和专业技术能力；
- 1.4 有依法缴纳税收和社会保障资金的良好记录；
- 1.5 参加政府采购活动前三年内，在经营活动中没有重大违法记录；
- 1.6 法律、行政法规规定的其他条件。

2. 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；

3. 根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库[2016]125 号）的规定，对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的供应商，拒绝参与本项目政府采购活动；【查询渠道：“信用中国”网站（www.creditchina.gov.cn）、

中国政府采购网 (www. ccgp. gov. cn)】;

4. 本项目不接受联合体。

三、投标人可在河南招标采购服务有限公司得到进一步的信息和查阅招标文件。

四、投标人可从 2018 年 04 月 14 日-2018 年 04 月 20 日起每天(法定公休日、节假日除外)8: 00-12: 00、14: 30-17: 30 时(北京时间)在河南招标采购服务有限公司购买招标文件, 本招标文件每套售价为 300 元人民币, 售后不退。

注意事项: 购买招标文件时需提供单位授权委托书(原件)、被授权人身份证原件及复印件、营业执照副本原件及复印件(加盖公章)。

五、所有投标文件应于 2018 年 05 月 04 日 8: 00-9: 00 时(北京时间)由专人递交到河南招标采购服务有限公司四楼开标大厅。

六、定于 2018 年 05 月 04 日上午 9: 00 时(北京时间), 在河南招标采购服务有限公司四楼开标大厅(第一会议室)公开开标。届时请参加投标的代表出席开标仪式。

七、其他事项

采购人: 郑州市教育局电化教育馆

地址: 郑州市南阳路 314 号

联系人: 王女士

联系电话: 0371-66995447

代理机构: 河南招标采购服务有限公司

联系地址: 郑州市纬四路 13 号(花园路与纬四路交叉口东 50 米路北)

项目联系人: 张先生

电 话: 0371-65950056

财务咨询电话: 0371-65955702

开户行: 广发银行郑州行政区支行

帐号: 8898516010005452

采 购 人: 郑州市教育局电化教育馆

招标代理机构: 河南招标采购服务有限公司

日 期: 2018 年 04 月 13 日

第二章 投标人须知

一. 说明

1. 适用范围

1.1 本招标文件仅适用于政府采购公开招标的货物及伴随服务。

2. 定义

2.1 采购人：“招标项目资料表”中所述的、依法进行政府采购的国家机关、事业单位、团体组织。

2.2 采购代理机构：受采购人委托组织招标活动，在招标过程中负有相应责任的社会中介组织。

2.3 合格投标人：满足本项目“招标公告”和“招标邀请”中资格条件要求的投标人。

2.4 中标人：接到并接受中标通知，最终被授予合同的投标人。

2.5 投标文件：指投标人根据招标文件要求提交的所有文件。

2.6 供应商：有能力向采购人提供货物及伴随服务的法人、其他组织或者自然人。

2.7 货物：指除了咨询服务以外的所有的物品、设备、装置和/或包括附件、备品备件、图纸、技术文件、用于运输和安装的包装、培训、维修和其他类似服务的供应。

3. 投标费用

3.1 无论投标过程中的作法和结果如何, 投标人应自行承担所有与准备和参加投标有关的全部费用, 采购人和采购代理机构在任何情况下均无义务和责任承担上述费用。

二. 招标文件

4. 招标文件的构成

4.1 招标文件用以阐明本次招标的货物和服务要求、招标投标程序和合同条件。

4.2 招标文件由下述部分组成：

第一卷

第一章 招标邀请

第二章 投标人须知

第三章 合同基本格式

第四章 投标文件通用格式

第二卷

第五章 招标项目资料表

- 第六章 合同专用条款资料表
- 第七章 招标项目需求及技术规格要求
- 附件： 评标标准和评标方法

(以实际内容为准)

4.3 投标人应仔细阅读招标文件中投标人须知、条款、格式和技术规范等所有事项，按招标文件的要求制作并提交投标文件，并保证所提供的全部资料的真实性，以使其投标对招标文件做出实质性响应，否则，将承担其投标被拒绝的风险。

4.4 招标文件包含第一卷和第二卷，投标人制作投标文件时应充分完整理解招标文件的整体要求。如果第一卷和第二卷对同一事项的描述有冲突或矛盾，除非采购人或采购代理机构另有解释，均以第二卷为准。

5. 招标文件的澄清

5.1 任何对招标文件认为有需要澄清的疑问的潜在投标人，均应在自购买招标文件之日起七个工作日内，以书面方式（加盖公章且法人代表（负责人）或其授权代表人签字的原件，下同）以书面形式一次性通知到采购人和采购代理机构。采购人和采购代理机构对潜在投标人在规定期限内提交的疑问将以书面方式予以答复，同时有可能将不标明疑问来源的书面答复函发至所有潜在投标人。在规定的时间内未提出疑问的，将被视为对招标文件完全认可。开标后，采购人和采购代理机构不接受任何对招标文件内容的质疑。

6. 招标文件的修改

6.1 在投标截止日期十五（15）日前，采购人和采购代理机构可主动或在解答投标人提出的澄清问题时对招标文件进行修改。

6.2 以上修改或延长投标截止时间和开标时间的通知将在投标邀请函所述投标截止日期三（3）日前，以书面方式通知到所有已购买招标文件的潜在投标人，并构成招标文件的一部分，对所有投标人均具有约束力。

6.3 投标人在收到上述通知后，应立即向采购人和采购代理机构回函确认。

6.4 为使投标人有充分的时间对招标文件的修改部分进行研究，采购人和采购代理机构可适当延长投标截止期。

三. 投标文件的编写

7. 投标的语言

7.1 投标文件以及投标人与采购人和采购代理机构就有关投标的所有往来函件均应使用中文。投标人提供的外文资料应附有相应的中文译本，并以中文译本为准。

8. 投标文件计量单位

8.1 除在招标文件的技术文件中另有规定外，计量单位均使用中国公制计量单位。

9. 投标文件的组成

9.1 投标文件格式（未标注固定格式的均非强制格式要求）详见第四章，未提供格式的，投标人可自行设计。

9.2 参加投标的投标人应认真阅读并理解本招标文件，按要求编制投标文件。投标文件要字迹清晰、不得涂改，按要求加盖公章和签字。

9.3 投标文件应按 A4 纸打印并装订成册。

9.4 投标人提供的全部资料必须准确详实。投标人的相关资质或其他情况如果没有按要求提供具体证明材料，将可能构成不中标的原因。

9.5 招标文件中的每个分包，是项目招标不可拆分的最小投标单元，拆包投标将视为漏项或非实质性响应不予接受。投标人如同时投标多包，可提交一套资格证明文件。

10. 投标格式

10.1 投标人应参照招标文件中提供的格式完整地填写相关内容，按招标文件要求提交资格证明文件。

11. 投标报价

11.1 投标人应参照招标文件提供的投标报价表格式填写提供各项货物及服务的单价、分项总价和投标总价。投标文件中报价出现前后不一致的，按照下列规定修正：（一）投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；（二）大写金额和小写金额不一致的，以大写金额为准；（三）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；（四）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。同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价经投标人的法定代表人或经其授权的投标人代表书面签字确认后产生约束力，投标人不确认的，其投标无效。

11.2 投标总报价应是采购人指定地点交货的包括交货前发生的各种 税费、运费及保险费、运杂费、以及伴随的其它服务费总报价。总报价分解为：设备和附属装置、备品备件和专用工具、卖方技术服务（安装、调试、运行）报价、采购人派员参加技术联络和工厂监造、检验、技术培训费用、运保费、各类税费及验收检测费，各项报价应准确填入投标报价表相应栏内。

11.3 投标人根据上述规定所作分项报价的目的只是为了评标时对投标文件进行比较的方便，但并不限制采购人订立合同的权力。

- 11.4 投标报价应完全包括招标文件规定的货物和服务范围，不得任意分割或合并所规定的分项。
- 11.5 投标人对每种货物和服务只允许有一个报价，采购人和采购代理机构不接受有任何选择性报价的投标。
- 11.6 投标人不得以任何理由在开标后对投标报价予以修改，报价在投标有效期内是固定的，不因任何原因而改变。任何包含价格调整要求和条件的投标，将被视为非实质性响应投标而予以拒绝。采用综合评分法时，最低投标报价并不意味着一定中标。

12. 投标货币

- 12.1 除非另有规定，投标人提供的所有货物和服务均应用人民币报价。
- 12.2 投标人提供从中华人民共和国境外取得的货物和服务应同时提供相应的 CIF/CIP 美元价格，该价格在任何情况下都不对约定投标货币产生影响。

13. 投标人资格证明文件

- 13.1 依据“招标项目资料表”中的要求按第四章投标文件通用格式提交相应的资格证明文件，作为投标文件的一部分，以证明其有资格进行投标和有能力履行合同。如果投标人是联合体，则联合体各方应分别提交资格文件、以及联合体协议，联合体协议应标明主办人。

14. 投标货物和服务符合招标文件技术要求的文件

- 14.1 投标人应提交证明其拟供货物和服务符合招标文件规定的技术响应文件，作为投标文件的一部分。
- 14.2 在主要设备（产品）规格一览表中说明货物的品牌型号、规格参数、制造商及原产地等。
- 14.3 招标文件中如有为简述货物品质、基本性能而标示的品牌或型号仅供投标人选择货物在质量、水平上的比照参考，不具有限制性。投标人可提供品质相同或优于同类产品的货物。
- 14.4 使用综合评分法的采购项目，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，按同品牌投标报价最低的投标人获得中标人推荐资格（若投标报价相同时，按技术规格响应程度最高的，若技术规格相同，则按售后服务最优的）。其他同品牌投标人不作为中标候选人。
- 14.5 非单一产品采购项目，采购人应当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 14.4 条的规定处理。
- 14.6 证明文件可以是文字资料、图纸和数据，并提供：
- 14.7 货物主要技术指标和性能的详细描述；
- 14.8 保证货物正常和连续运转期间所需的所有备件和专用工具的详细清单，包括其价格和供货来源资料；

15. 投标保证金

- 15.1 投标人应按“招标项目资料表”中规定的数额向采购代理机构提交投标保证金，但不得超过所投分包预算金额的百分之二。
- 15.2 投标保证金是为了保护采购人及采购代理机构避免因投标人的行为带来的损失。采购人及采购代理机构因投标人的行为受到损害时，可根据第 15.7 条的规定没收投标人的投标保证金。
- 15.3 投标保证金应以人民币计，应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。
- 15.4 未按规定提交投标保证金的投标，将被视为非实质性响应的投标予以拒绝。
- 15.5 未中标的投标人的保证金，将在中标通知书发出后五（5）个工作日内无息退还，但投标人必须向采购代理机构交回提交投标保证金时开具的财务票据。中标公告发布后，未中标的投标人即可至采购代理机构退还投标保证金。
- 15.6 中标的投标人的投标保证金，在采购人和中标人签订合同后五（5）个工作日内无息退还，或按照招标文件的规定转为履约保证金，或扣除采购代理机构中标服务费后无息退还差额。
- 15.7 下列任何一种情形发生时，投标保证金将被没收：
 - (1) 投标人在招标文件规定的投标有效期内撤回其投标；
 - (2) 投标人在投标文件中故意提供虚假材料；
 - (3) 中标人拒绝在中标通知书规定的时间内签订政府采购合同；
 - (4) 中标人未能按招标文件规定提交履约保证金（需要提交时）；

16. 投标有效期

- 16.1 投标文件应自投标规定的开标之日起，在“招标项目资料表”规定的时间内保持有效。投标有效期不足的投标将被视为非实质性响应，并予以拒绝。
- 16.2 在特殊情况下，在原投标有效期截止之前，采购人和采购代理机构可要求投标人延长其投标有效期。这种要求与答复均应以书面形式提交。投标人可以拒绝这种要求，其投标保证金不会被没收，但其投标在原投标有效期期满后将不再有效。同意延期的投标人将不会被要求和允许修正其投标，而只会被要求相应延长其投标保证金的有效期。在这种情况下，本须知第 15 条有关退还和没收投标保证金的规定在投标有效期的延长期内继续有效。

17. 投标文件的式样和文件签署

- 17.1 投标人制作“招标项目资料表”规定数目的投标文件正本和副本，每套投标文件应清楚地标明“正本”或“副本”。副本应与正本内容一致，若副本与正本存在文字或表述的不符之处，以正本为准。
- 17.2 投标文件及所有文件由投标人或经正式授权的代表在相应处签字，授权代表必须将以书面形式出

具的“法定代表人授权书”附在投标文件正本中。投标文件副本可以是正本完整的复印件。

17.3 任何行间插字、涂改和增删，必须由投标人签字人用姓或首字母在旁边签字或加盖公章后有效。

四. 投标文件的递交

18. 投标文件的密封和标记

18.1 为便于开标和唱标，投标人应将“开标一览表”在投标文件之外另行制作一份，单独密封并粘贴在正本的密封袋外边，并在单独密封袋上标明“开标一览表、所投包号、投标人名称”字样并加盖公章。如果投标文件中的报价与“开标一览表”报价之间有差异，以“开标一览表”中的报价为准，投标人应接受评标所进行的修正，并承担一切不利于投标人的后果。

18.2 投标人应将投标文件正本和副本装在密封袋中，在密封袋上标明“正本”或“副本”字样，并在封签处加盖公章。

18.3 密封袋上均应：

(1) 注明“招标项目资料表”中载明的项目名称、招标编号、包名、正本、副本及“在____年__月__日之前不得启封”字样。

(2) 写明投标人的名称。

18.4 如果密封袋上未按 18.2、18.3 要求密封和加写标记，采购人和采购代理机构对投标文件的保密性、误投或过早启封概不负责。对拆标后未装订成册的投标文件，投标人应承担可能被拒绝的风险。

18.5 投标人应清楚招标文件必须直接从采购代理机构购买获得，未经购买仅根据复制的招标文件编制的投标文件，或投标人名称与购买招标文件时登记的名称不一致的投标文件，均将被拒收。

19. 投标截止期

19.1 投标人应在不迟于“招标项目资料表”中规定的截止日期和时间将投标文件按照“招标项目资料表”中载明的地址递交至采购代理机构。

19.2 采购人和采购代理机构可以按第 6 条规定，通过修改招标文件自行决定酌情延长投标截止期限。在此情况下，采购人、采购代理机构和投标人受投标截止期制约的所有权利和义务均应延长至新的截止日期。

20. 迟交的投标文件

20.1 采购代理机构将拒绝并原封退回在第 19 条规定的投标截止期后收到的任何投标文件。

21. 投标文件的修改和撤回

21.1 投标人在递交投标文件后，在投标截止时间之前可以修改或撤回其投标文件，但投标人必须在投标截止时间之前将修改或撤回的书面通知递交至采购代理机构。

- 21.2 投标人的修改或撤回通知书应按第 18 条规定编制、密封、标记和递交。
- 21.3 在投标截止期之后，投标人不得对其投标做任何修改。
- 21.4 从投标截止期至投标人在投标文件中载明的投标有效期满期间，投标人不得撤回其投标，否则其投标保证金将按照第 15 条的规定被没收。

五. 开标与评标

22. 开标

- 22.1 采购代理机构在“招标项目资料表”中规定的日期、时间和地点组织公开开标。开标时邀请所有投标人派代表参加。
- 22.2 开标时，应当由投标人或者其推选的代表检查投标文件的密封情况；经确认无误后，由采购人或者采购代理机构工作人员当众拆封，采购代理机构当众宣读投标人名称、修改和撤回投标的通知、投标价格、折扣声明以及采购人和采购代理机构认为必要的内容。
- 22.3 在开标时没有启封和读出的投标文件（包括按照第 21 条递交的修改书）将原封退回投标人。
- 22.4 开标过程应当由采购人或者采购代理机构负责记录，由参加开标的各投标人代表和相关工作人员签字确认后随采购文件一并存档。投标人代表对开标过程和开标记录有疑义，以及认为采购人、采购代理机构相关工作人员有需要回避的情形的，应当场提出询问或者回避申请。采购人、采购代理机构对投标人代表提出的询问或者回避申请应当及时处理。投标人未参加开标的，视同认可开标结果。
- 22.5 开标时，因投标人未在投标文件封装上注明或标注不清晰所投包号而被公开唱标的各包投标报价，但评标时发现其中有包因投标人数不足三家而废标的，由此造成的风险和后果由投标人自行承担，采购代理机构对唱标内容和过程不承担责任。
- 22.6 开标结束后，采购人或者采购代理机构应当依法对投标人的资格进行审查。资格审查合格的进入评标环节。

23. 评标工作

- 23.1 评标工作由评标委员会（下称评委会）主持对所有投标人的投标文件进行审评，并按综合评分由高到低的顺序推荐出“招标项目资料表”中载明数量的中标候选人。
- 23.2 评委会成员为 5 人以上单数经济、技术专家和采购人代表组成，其中除采购人代表以外的外聘专家不少于三分之二，并按政府采购制度的规定从政府采购专家库中随机抽取产生。

24. 投标文件的澄清

- 24.1 为了有助于对投标文件进行审查、评估和比较，评委会会有权向投标人质疑，请投标人澄清其投标

内容。投标人有责任按照采购代理机构通知的时间、地点、方式由投标人或其授权代表进行答疑和澄清。

24.2 重要澄清的答复应是书面的，并由投标人法定代表人或其委托代理人签字。

24.3 投标人的澄清文件是投标文件的组成部分，并取代投标文件中被澄清的部分。

24.4 投标文件的澄清不得对投标内容进行实质性修改。

25. 投标文件的符合性审查

25.1 评委会将审查投标文件是否完整、文件签署是否合格、投标人是否提交了投标保证金、有无计算上的错误等。

25.2 价格计算错误的按照第 11.1 项处理。

25.3 允许修正投标文件中不构成重大偏离的、微小的、非正规的、不一致或不规则的地方。

25.4 在对投标文件进行详细评估之前，评委会将确定每一投标是否对招标文件的要求做出了实质性的响应，而没有重大偏离。实质性（标注*条款）响应的投标是指投标符合招标文件的所有条款、条件和规定且没有重大偏离和保留。

25.5 评委会判断投标文件的响应性仅基于投标文件本身内容而不靠外部证据。

25.6 评委会将依据投标人提供的证明文件审查投标人的商务、技术和生产能力。如果确定投标人无资格和能力履行合同，其投标将被拒绝。

25.7 实质上没有响应招标文件要求的投标将被拒绝，投标人不得通过修正或撤消不符之处而使其投标成为实质上响应投标。

25.8 评标中有下列情形之一的，其投标将会被拒绝：

- (1) 投标人提交保证金不符合招标文件要求的；
- (2) 投标报价超出采购预算或最高限价的；
- (3) 资格证明文件不全，或不满足招标文件要求的；
- (4) 投标有效期不足的；
- (5) 投标文件附有采购人不能接受的条件；
- (6) 不符合招标文件中规定的其他实质性要求。

26. 投标的评价

26.1 评委会审查、评价投标文件是否符合招标文件的商务、技术等实质性要求；只对已判定为实质性响应的投标文件进行评价和比较。

26.2 评审因素的设定应当与投标人所提供货物服务的质量相关，包括投标报价、技术或者服务水平、履约能力、售后服务等。资格条件不得作为评审因素。

- 26.3 评标时，评标委员会各成员应当独立对每个投标人的投标文件进行评价，并汇总每个投标人的得分。
- 26.4 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。
- 26.5 评标委员会成员对需要共同认定的事项存在争议的，应当按照少数服从多数的原则作出结论。持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告。

27. 综合评标的确定

- 27.1 综合评标法，是指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由高到低的顺序推荐出“招标项目资料表”中载明数量的中标候选人。

28. 保密及其它注意事项

- 28.1 评标是招标工作的重要环节，评标工作在评委会内独立进行。评标委员会成员名单在评标结果公告前应当保密。
- 28.2 评委会将遵照规定的评标方法，公正、平等地对待所有投标人。
- 28.3 在开标、评标期间，投标人不得向评委询问评标情况，不得进行旨在影响评标结果的活动。否则，其投标可能被拒绝。
- 28.4 为保证评标的公正性，开标后直至授予投标人合同，评委不得与投标人私下交换意见。
- 28.5 在评标工作结束后，凡与评标情况有接触的任何人员不得擅自将评标情况扩散出评标人员之外。
- 28.6 评委会和采购代理机构不退还投标文件。

六. 授予合同

29. 合同授予标准

- 29.1 除第 32 条的规定之外，采购人和采购代理机构将把合同授予被确定为实质上响应招标文件要求并有履行合同能力的评分最高的投标人。

30. 评标时更改采购货物和服务数量的权力

- 30.1 采购人和采购代理机构在授予合同时有权在“招标项目资料表”规定的范围内，对招标文件第二卷中规定的设备和服务的数量予以增加或减少，但不得对货物、单价或其它的条款和条件做任何改变，且增减数量不得超过招标文件规定数量的百分之十。

31. 评标结果的公告

- 31.1 采购代理机构应当在评标结束后两个工作日内将评审报告送采购人。采购人应当在收到评审报告

后五个工作日内，按照评审报告中推荐的中标候选供应商顺序确定中标人。

31.2 自采购人按规定确定中标供应商之日起两个工作日内，采购代理机构应将中标结果以中标公告形式在省级政府采购管理部门指定的媒体上予以发布，同时向中标供应商发出中标通知书。

31.3 各有关当事人对中标结果有异议的，可以在中标结果公告期限届满之日起七个工作日内，书面形式一次性同时向采购人和采购代理机构提出质疑(加盖单位公章且法人签字)，由法定代表人或其授权代表携带企业营业执照复印件(加盖公章)及本人身份证件(原件)一并提交(邮寄、传真件不予受理)，并以质疑函接收日期作为受理时间。逾期提交或未按照要求提交的质疑函将不予受理。

32. 接受和拒绝任何或所有投标的权力

32.1 如出现重大变故，采购任务取消情况，采购人和采购代理机构保留因此原因在授标之前任何时候接受或拒绝任何投标、以及宣布招标无效或拒绝所有投标的权力，对受影响的投标人不承担任何责任。

33. 中标通知书

33.1 在投标有效期满之前，采购代理机构将以书面形式通知中标人中标。

33.2 中标通知书将作为进行合同谈判和签订合同的依据。

34. 签订合同

34.1 中标人应按中标通知书指定的时间、地点，与采购人进行合同谈判。

34.2 招标文件、中标人的投标文件和澄清文件等，均应作为签约的合同文本的基础。

34.3 如采购人或中标人拒签合同，则由政府采购管理部门依据政府采购法规制度的规定对违约方做出行政处罚。

34.4 如中标人不按第 34.2 条约定谈签合同，采购人和采购代理机构将报请取消其中标决定，并没收其投标保证金。采购人和采购代理机构可在候选中标单位中按顺序重新选定中标单位。

35. 履约保证金

35.1 中标人应按照招标文件或合同条款的规定，采用招标文件中提供的履约保函格式、政府采购履约担保函格式或采购人可以接受的其他形式向采购人提交履约保证金。

36. 其他

36.1 本招标文件第一卷由河南招标采购服务有限公司负责解释。

第三章 合同基本格式（参考）

合 同

编号：（招标编号）

甲方：郑州市教育局电化教育馆

乙方：

根据河南招标采购服务有限公司所签发的“**项目”的中标通知书和招标文件以及乙方投标文件，经甲乙双方协商，就甲方向乙方采购***项目（以下简称本项目）相关事宜达成一致意见，现签订本合同内容如下：

一、项目概况

1.1 项目名称：

1.2 项目地点

1.3 项目主要内容：

二、采购设备明细

2.1 设备清单：

甲方采购的设备清单详见本合同附件《设备分项报价一览表》

2.2 合同价款：

本合同第 2.1 款中全部设备的合同价款共计___元（大写： 元整），该合同价款中已包含甲方购买的全部设备及所有相关产品价款、运输费用、安装调试费用、培训费用、服务费用、税金及乙方合理利润等一切相关费用。

三、合同价款的支付

内容：***

四、交付

4.1 交付时间：乙方须自本合同签订之日起 60 个日历天内甲方交付本项目全部设备。

4.2 交付地点：甲方指定地点。

4.3 交付方式：乙方负责自费将设备送达至甲方指定交付地点并完成安装、调试。不可抗力原因造

成的中途耽搁，乙方应将就有关情况尽快告知甲方。

五、验收

5.1 本项目完工并验收条件后，乙方须按项目验收有关规定向甲方提交完整验收资料。

5.2 甲方应在其交付的设备安装、调试完成并正常运行之日起 15 日内组织有关专家进行验收、填写设备验收证明，并应将该设备验收证明交付郑州市人民政府采购办公室和乙方为付款依据。

六、甲方权利与义务

6.1 甲方负责协调本项目各种工作。

6.2 甲方负责协调各相关部门配合乙方实施本项目。

6.3 甲方应按照本合同约定支付合同款项。

七、乙方权利与义务

7.1 乙方指定代表___（职务：销售助理，联系电话：_____）处理关于本项目与甲方一切相关的业务事宜，并保证本项目的整个实施过程及时、安全。

7.2 乙方须向甲方提供软件开发、硬件集成、软硬件实施部署等工作计划，并按照甲方确认的计划开展工作。

7.3 乙方须严格按照招、投标文件要求实施本项目。

7.4 乙方负责项目资料整理、归档工作并向甲方移交项目资料。

7.5 乙方保证按投标文件、甲方业务需求提供本次项目所需软、硬件产品及维修服务等。

八、培训及售后服务

乙方须按照本合同附件三《售后服务承诺书及客户培训计划》及招、投标文件中相关要求为甲方提供培训及售后服务。

九、违约责任

9.1 乙方所提供设备及软件的性能、技术标准等不符合招、投标文件及本合同规定的，甲方有权视具体情况解除本合同，届时，乙方除须退还甲方已付全部合同价款外，并须按照本合同第 2.2 款约定的合同价款金额 20% 的标准向甲方支付赔偿金，甲方实际产生的损失超过前述金额的，乙方并须另行赔偿。

9.2 除不可抗力及甲方因素外，乙方未在本合同规定的期限内完交付的，每逾期一日，须按照本

合同第 2.2 款约定的合同价款金额 3%的标准向甲方支付逾期违约金；拖延超过三个月时，甲方并有权视具体情况解除本合同，届时，乙方除须退还甲方全部已付合同价款外，并须按照本合同第 2.2 款约定的合同价款金额 20%的标准向甲方支付赔偿金，甲方实际产生的损失超过前述金额的，乙方并须另行赔偿。

9.3 除乙方原因或不可抗力因素外，甲方逾期支付合同款项的，每逾期一日，须按照本合同第 2.2 款约定的合同价款金额 0.1%的标准向乙方支付逾期违约金。

9.4 甲方无正当理由拒绝验收的，须按照本合同第 2.2 款约定的合同价款金额 3%的标准向乙方支付违约金；逾期超过三个月未验收的，乙方并有权解除本合同。

9.5 如因乙方设备或软件致使甲方受到第三方追究侵犯其专利权、商标权、著作权或其他知识产权法律责任的，乙方应赔偿由此造成的全部甲方损失（含律师费、诉讼费等）；如因此影响甲方正常使用设备的，按本合同 9.2 款约定处理。

十、合同文件及解释顺序

10.1 组成本合同的文件及解释顺序为：招标文件、中标通知书；本合同及补充条款、投标书及其附件；标准、规范及有关技术文件。

10.2 合同履行过程中，甲方、乙方有关本项目的洽商、变更等书面协议或文件视为本合同的组成部分。

十一、合同生效及其他

11.1 本合同未尽事宜由甲乙双方另行协商并签订书面补充协议。

11.2 发生争议双方协商解决不成的，由甲方所在地人民法院管辖。

11.3 本合同经双方代表签字并盖章后生效。

11.4 本合同一式陆份，甲方执肆份，乙方执贰份，均具有同等法律效力。

甲方：郑州市教育局电化教育馆 乙方：_____ 代表人：

地址：河南省郑州市南阳路 314 号 地址：_____ 代表人：

签订日期：2018 年 月 日

合同附件：1、设备分项报价一览表；2、主要设备（产品）规格一览表；3、售后服务承诺书及培训计划。

第四章 投标文件通用格式

1. 法定代表人授权书

本授权书声明：注册于（注册地址名称）的（投标人全名）的在下面签字的（法定代表人姓名、职务）代表本公司授权（单位名称）的在下面签字的（被授权人的姓名、职务）为本公司的合法代理人，就招标编号为_____（项目名称）的投标及合同执行，以本公司名义处理一切与之有关的事务。

本授权书于____年__月__日签字生效，特此声明。

后附法定代表人及被授权人身份证复印件

法定代表人签字或盖章：

被授权人签字：

被授权人职务：

单位名称（公章）：

2. 投 标 书

致：（采购代理机构名称）

根据贵方的投标邀请（招标编号），签字代表（全名、职务）经正式授权并代表投标人（投标人名称、地址）提交下述文件正本一份和副本___份，并对之负法律责任。

1. 法定代表人授权书
2. 开标一览表
3. 资格证明文件
4. 投标报价表格
5. 技术规格/商务条款偏差表
6. 投标人资格证明文件
7. 按招标文件投标人须知和商务技术条款要求提供的其他有关文件
8. 金额为人民币_____元投标保证金

据此函，签字代表宣布同意如下：

1) 所附投标报价表中规定的应提供的项目投标总价为人民币_____，（大写）_____。

2) 如果我们的投标文件被接受，我们将按招标文件的规定签订并严格履行合同中的责任和义务。

3) 投标人已详细审查全部招标文件，包括修改文件以及全部参考资料和有关附件。我们完全理解并同意放弃对这方面有不明及误解的权力。

4) 本投标自开标日起有效期为___天。

5) 如果在规定的开标时间后，投标人在投标有效期内撤回投标，其投标保证金将被贵方没收。

6) 投标人承诺，与招标方聘请的为此项目提供咨询服务及任何附属机构均无关联，非招标方的附属机构。

7) 投标人同意提供按照贵方可能要求的与其投标有关的一切数据或资料，完全理解贵方不一定接受最低价的投标或收到的任何投标。

投标人代表签字：

电话：

投标人名称（公章）：

邮政编码：

日 期：

3. 资格证明文件

- 1) 投标人应如实填写和提交下述规定表格以及其他有关资料。
- 2) 所附格式中要求填写的全部问题和/或信息都必须填写。
- 3) 本资格声明的签字人应保证全部声明和填写的内容是真实的和正确的。
- 4) 评标将根据投标人提交的资料判断其履行合同的合格性及能力。
- 5) 投标人提交的材料将被保密，但并不退还。
- 6) 全部文件应按“招标项目资料表”规定的语言和份数提交。

3.1 投标人资格申明信

致：（采购代理机构名称）

为响应你方于____年__月__日发出的（招标编号）投标邀请，下述签字人愿意参加投标，提供招标文件中货物/服务报价表规定的（项目/货物名称），递交下述文件并保证所有陈述是正确的和真实的。

1. 投标文件正本一份，副本____份。写明我方有权代表制造厂家的货物投标。（当投标人为代理贸易公司时填写）。

2. 我方的资格申明，正本一份，副本____份。

3. 签署人保证资格文件的陈述真实正确的证明。

投标单位

被授权投标代表人

名称：

签名：

地址：

职位：

邮编：

电话：

3.2 投标人资格申明

一 基本情况

- 1) 投标人名称
- 2) 地址
联系电话、传真
- 3) 成立或/注册日期（提供其营业执照副本复印件）
- 4) 法定代表人
- 5) 制造商名称和地址（如有）
- 6) 投标人所属的集团/财团公司
- 7) 投标人员工总人数：
其中：高级职称人数： 中级职称人数：
 管理人员人数： 技术人员人数：
- 8) 投标联系人
联络方式及电话：

二 财务状况

- 1) 固定资产
- 2) 流动资产
- 3) 长期负债
- 4) 流动负债
- 5) 资产净值
- 6) 有关开户银行的名称、地址
- 7) 最近三年每年的营业总额

年份	业务总额	国内	出口

- 8) 最新资产负债表：由会计事务所审核的最近一年的财务报表。

三 供应投标货物经验（业绩）

- 1) 最近三年销售记录
- 2) 成功运行两年以上的供货合同
- 3) 近三年中类似货物最终用户单位

名称	签约	货物名称	销售	合同额
----	----	------	----	-----

地址	日期	及型号	数量	

4) 最终用户出具的证明

5) 业绩要求见第二卷

兹证明以上陈述是真实的、准确的，所提供的资料和数据均已提供，我们同意按贵方要求出示有关证明文件。

日 期： _____

投标人名称： _____

授权代表签字： _____

授权代表职务： _____

电话及传真号码： _____

3.3 证书

下述签字人证明本资格文件和要求的格式中的说明是真实的和正确的。

下述签字人在此授权并要求任何被征询的机构向招标公司提供招标文件所要求的资料，以证明本声明及本公司实力和信誉。

下述签字人理解并同意提交对其他有关资格材料的进一步要求。

投标单位

被授权投标代表人

名称：

签名：

地址：

职位：

邮编：

电话：

4. 投标报价表格

4.1 开标一览表

投标人：（此处填名称并盖章）

单位：人民币元

项目包号	投标总价	投标保证金	投标的主要 设备品牌型号	产地	其他声明

投标人授权代表签字：

说明：

1. 与本表同时公开唱标的内容包括对其投标文件的修改或撤回通知、投标价折扣声明、其他采购人认为应该宣读的内容等。

2. 本表为唱标用，加盖公章并签字有效，按投标人须知中要求单独密封提交一份。

4.2 主要设备分项报价一览表

投标人：（此处填名称并盖章）

项 目：（此处填包号和名称）

金额单位：元

序号	设备名称	品牌型号	单位	数量	单价	小计	运输及保险费	技术服务费	税费	合计	交货日期	交货地
合计												

投标人授权代表签字：

说明：1、技术服务费是指安装、调试、运行等费用。

2、税费主要指非国产货物的关税及其他费用等。

5. 技术规格和商务条款偏差表

投标商：（此处填名称）

项 目：（此处填包号和名称）

序号	设备名称	技术参数及要求		对招标 文件偏差	描 述	备注
		招标文件	投标文件			
1	名称 1					
	参数名称 1					
	参数名称 2					
					
2	名称 2					
	参数名称 1					
	参数名称 2					
					
					

投标人（盖章）：

授权代表（签字）：

注明：投标设备或商务条款存在偏差的必须如实填写本表，否则可能导致投标不被接受。

6. 售后服务计划及承诺

投标人必须提供但不限于提供以下内容：

1. 详细说明售后服务的内容、形式、含免费维修时间、解决质量或操作问题的响应时间、解决问题时间、维修单位名称、地点。
2. 技术培训、质量保证措施。
3. 该项目所提供的其它免费物品或服务。

投标单位公章：

日期：

投标人代表签字：

职务：

7. 投标人及投标产品简介

投标人必须但不限于提供以下内容：

1. 投标人简介：包括公司概况、组织机构、近三年经营情况、技术设备、人员状况等；

2. 质量保证体系和质量认证证明；

3. 投标产品详细介绍（需提供详细、有效证明文件）；

4. 业绩及目前正在执行合同的情况；

。

投标单位公章：

投标人代表签字：

日期：

职务：

8. 投标人资格证明文件

1. 供应商营业执照复印件；
2. 2017 年度财务审计报告复印件；
3. 依法缴纳税收和社会保障资金的相关材料复印件；
4. 在“信用中国”网站中查询“失信被执行人”和“重大税收违法案件当事人名单”（<http://www.creditchina.gov.cn/>），以及在“中国政府采购网”网站（www.ccgp.gov.cn）中查询“政府采购严重违法失信行为记录名单”共 3 项的查询结果网页扫描件。
5. 投标保证金缴纳凭证。
6. 反商业贿赂承诺书；
7. 最近三年内，在经营活动中没有重大违法、违纪行为书面声明函；

第二卷

第五章 招标项目资料表

本表关于要采购的货物的具体资料是对投标人须知的具体补充和修改，如有矛盾，应以本资料表为准。此投标资料表带“*”的为投标人必须满足的商务条件，如不满足，可能导致无效投标或投标不予接受。

条款号	内 容
说 明	
1	采购人名称：郑州市教育局电化教育馆
2	招标代理机构名称：河南招标采购服务有限公司 电话：0371-65950056
3	<p>*投标资格要求：</p> <ol style="list-style-type: none"> 1. 具有独立承担民事责任的能力； 2. 具有最近一年度的财务审计报告； 3. 具有依法缴纳税收和社会保障资金的相关材料； 4. 参加政府采购活动前三年内在经营活动中没有重大违法、违纪行为的书面声明； 5. 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； 6. 根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库[2016]125号）的规定，对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的供应商，拒绝参与本项目政府采购活动；【查询渠道：“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）】； 7. 本项目不接受联合体。
4	投标语言：中文，投标人提供的外文资料应附有相应的中文译本
投 标 报 价 和 货 币	

5	<p>投标报价为：目的地交货价（含税、安装调试、运杂费等工程所需费用）。 相关费用（由中标人承担的费用）：包括中标服务费、税费、清关、银行手续费、安装、调试、运保、装卸费、培训、售后服务等相关费用。</p> <p><u>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。</u></p> <p>中标服务费：向中标单位收取<u>贰万元</u>中标服务费。</p>
6	<p>投标货币：人民币</p>
<p>投 标 书 的 编 制 和 递 交</p>	
7	<p>资格证明文件：</p> <ul style="list-style-type: none"> *1. 投标供应商营业执照副本复印件（加盖公章）； *2. 法人授权书； *3. 提供 2017 年度财务审计报告复印件； *4. 依法缴纳税收和社会保障资金的相关材料复印件（至少应提供 2017 年 5 月 1 日以来任 1 个月的缴纳税收和社保基金的证明材料）； *5. 参加政府采购活动近 3 年内在经营活动中没有重大违法记录的书面声明承诺并加盖单位公章原件装订进投标文件正本； *6. 反商业贿赂承诺书； *7. 根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库[2016]125 号）的规定，对列入失信被执行人、重大税收违法案件当事人名单查询结果网页打印件加盖公章【查询渠道：“信用中国”网站（www.creditchina.gov.cn）】；政府采购严重违法失信行为记录名单的查询结果网页打印件加盖公章【中国政府采购网（www.ccgp.gov.cn）】。
8	<p>业绩要求：（详见评分标准，以评分标准业绩要求为准。）</p>
9	<p>货物技术证明文件：</p> <p>1. 投标人必须提供详细描述主要产品性能特点的原厂商技术文件、厂家正规彩页及产品说明资料供评标参考，并保证这些技术证明材料与投标货物的真实功能、性能参数的一致性；否则视为技术不满足；</p>

	<p>(投标人技术证明文件如未提供或不满足, 则视为技术不满足, 给予技术扣分处理。)</p> <p>*2. 国家实施生产许可证管理的产品应提供生产许可证 (提供复印件)。已列入国家强制性产品认证的产品应提供通过国家 3C 认证的有关证明材料;</p> <p>*3. 投标产品中如有政府采购强制采购产品的, 必须在财政部和国家发展改革委联合下发的最新一期节能产品政府采购清单之内, 并提供相关的证明文件, 不是最新一期的节能产品清单中的产品, 投标将视为无效投标。(提供政府采购节能清单文件首页、产品清单所在页和国家主管机构网站节能产品查询 http://www.ccgp.gov.cn/search/jnqdchaxun.htm 结果打印页等证明材料, 并加盖投标人公章);</p> <p>4. 其他政府采购政策功能体现见“附件: 评标标准和评标办法”要求;</p> <p>5. 投标货物的制造、安装和检验标准;</p> <p>6. 按技术规格规定提供备件和专用工具清单。</p> <p>7. 质保期外运行所需的随机备件、备品备件和易损件, 应详细列出名称、规格、数量及单价。</p>
10	<p>*投标保证金金额: 采购预算的 2%;</p> <p>*缴纳形式: 投标保证金应当以转账或者金融机构、担保机构出具的保函等非现金形式提交。(投标截止时间前必须到达招标机构银行帐户)。投标文件中需附招标代理机构出具的保证金收据或转账凭证(提供转账凭证须另附基本户证明)。接收保证金银行账户信息如下:</p> <p style="padding-left: 40px;">开户行: 广发银行郑州行政区支行</p> <p style="padding-left: 40px;">户名: 河南招标采购服务有限公司</p> <p style="padding-left: 40px;">帐号: 8898516010005452</p> <p>投标保证金应在投标有效期截止日后(20)天内有效。</p>
11	*投标有效期: 从开标之日起 60 天。
12	投标文件递交: 正本份数: 壹份, 副本份数: 肆份, 且正本和副本内容

	必须一致（投标文件副本可为正本完整的复印件），投标文件正本单独密封；所有副本可一起密封；开标一览表用信封单独密封；投标文件电子文档用信封单独密封。开标前开标一览表、电子档与正本粘在一起密封提交，副本叁份也同时密封提交。
13	投标文件递交至：开标大厅
评 标	
14	中标候选人推荐数量：按照有效投标人得分从高到低的顺序推荐 <u>壹名</u> 评标方法：综合评分法，见附件： 评分标准
15	交货期：所有产品交货日期为合同签订之日起 60 日内。 付款方式：主要设备到达指定地点后，并验收合格之后支付合同价款的 95%，自验收合格并向甲方交付使用之日起连续正常运行 90 日后，支付剩余合同价款的 5%。
授 予 合 同	
16	合同将授予综合得分最高的投标人。
17	合同数量增减范围：≤10%。

第六章 合同条款资料表

本表关于要采购的货物的具体资料是对合同条款的具体补充和修改，如有矛盾，应以本资料表为准。

序号	内容
1	买方名称：郑州市教育局电化教育馆 交货地点：用户指定地点
2	履约保证金金额：
3	备品备件要求：投标人自行承诺。
4	应提供的服务（包括但不限于以下内容）： 1、中标方必须具有售前售后技术服务的能力。 2、凡系统出现故障应 12 小时内到场，24 小时内解决问题。
5	验收及付款程序： 1、验收：需方在供方所交的货物安装、调试，正常运行 15 日内进行验收，填写设备验收证明。由中标方将验收证明一式五份上报郑州市教育局电化教育馆，由郑州市教育局电化教育馆组织有关专家进行复验，复验合格后，交郑州市人民政府采购办公室和中标方作为付款依据。 2、付款：主要设备到达指定地点并验收合格之后，需方向供方需支付合同价款的 95%，；验收合格并向需方交付使用之日起连续正常运行 90 日后，剩余合同价款的 5%作为质保金，由需方向供方一次性无息支付。

第七章 招标项目需求及技术规格要求

一、项目需求

货物需求一览表

项目编号	货物名称	单位	数量	完工期	交货地点
1	教育应用安全态势感知平台及应急支撑	批	1	合同生效后 60 日内完成设备安装、调试、运行。	郑州市教育局电化教育馆
2	郑州教育管理公共服务数据安全防护	批	1	合同生效后 60 日内完成系统安装、调试、运行。	
3	郑州教育数据中心重要信息系统安全服务	批	1	合同生效后 60 日内完成系统评测、定级、修复等。	
4	郑州市市直学校网站安全监测项目	套	1	合同生效后 60 日内完成系统安装、调试、运行。	

本次采购项目共分为一个包。

核心产品包括项目 1：教育应用安全态势感知和通报预警平台；项目 2：数据库防火墙产品。

二、技术参数

项目 1：教育应用安全态势感知平台项目

1、业务需求

郑州教育云计算中心信息化网络目前部署有杭州安恒明鉴网站安全监测平台，平台实现网站代码安全检测、网页内容安全监测、网站服务质量监测，为郑州教育网站提供全方位、全天候的安全监测服务，部署有绿盟科技 Web 应用防火墙，通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为教育 Web 应用提供保护，这些专业的安全防护设备逐渐达到了单位的防护屏障，从多个不同的角度满足了企业的安全防护需求。为发挥各类防护设备的综合防护价值，应对使用新型的攻击手段，提供有效的安全分析模型和管理工具来融合这些数据，可准确、高效地感知整个网络的安全状态以及发展趋势，从而对网络的资源做出合理的安全加固，对外部的攻击与危害行为可以及时的发现并进行应急响应，从而有效的实现防外及安内，保障信息系统安全，满足市局属网站、市直学校网站、局属信息系统和学校重点应用的本地化安全监测、等保监管等，2017 年上线了安全态势感知平台基础模块，包括预警通报、安全监测接口、通报预警处置和数据处理汇总，为进一步提升安全态势感知能力，提出安全态势感知平台项目（二期）建设。

2、产品需求一览表

序号	名称	单位	数量
1-1	网站立体监控平台	套	1
1-2	互联网域名安全巡管系统	套	1
1-3	互联网边界安全监测分析系统	套	1
1-4	教育应用安全态势感知和通报预警平台（二期）	套	1
1-5	安全应急支撑服务	年	1

3、技术参数

1-1 网站立体监控平台

分项指标	技术参数、功能要求及具体配置
基本要求	<p>基于互联网，利用安全的软硬件一体化封装原厂设备，采用直接或代理连接的检测方式，对一批网站远程进行实时监测与漏洞扫描，监测网站信息变动情况及响应速度，发现网站已存在的挂马、暗链、敏感内容和潜在的脆弱性等不安全因素。同时，要支持根据 IP 批量反查域名，支持常见 WEB 容器的日志分析。</p>
技术要求	<p>1. 设备特性 2U 机架式 X86 架构加固定制国产服务器，处理器不低于 Intel Xeon E5 系列；内存不低于 16GB，硬盘不低于 1TB SATA。 接口：2 个 10/100/1000M 网络接口。</p> <p>2. 软件架构要求 无需在被监测网站上安装代码或更改配置，采用 B/S 设计架构支持通过浏览器远程对产品进行使用，系统支持单机及集群式部署，支持各个设备间任务的负载均衡和任务集中调度。</p> <p>3. 系统知识库要求 要求拥有 1000 条以上的漏洞知识库，并且支持国家信息安全漏洞库（CNNVD）、支持国际 CVE 漏洞库。</p> <p>4. 扫描功能要求 4.1 检测对象：安全检测支持常见的 Web 服务容器。支持第三方应用漏洞检测。 4.2 检测引擎 可以动态分析出 Flash 内嵌的 URL 链接地址； 支持基于 Basic、NTLM 等认证方式的 Web 应用系统安全扫描； 支持预登录或指定 Cookie，对于某些需要特定权限才能访问的网页，可以先登录网站再进行检测； 支持自定义网站检测的入口地址； 支持同时对 30 个及以上的网站进行检测； 支持线程池机制，多线程并发爬取网页； 支持自定义检测深度，可选择无限制进行全站检测； 支持设置检测最大页面数量，可检测单网站 30 万页面以上数量级； 支持设置 HTTP 代理； 能够过滤重复页面，提高检测速度；</p>

分项指标	技术参数、功能要求及具体配置
	<p>支持基于 HTTP 和 HTTPS 协议的应用系统检测；</p> <p>支持错误页面特征匹配，精确判断网页是否返回正常，提高检测效率，如识别各种 404、500 等错误页面；</p> <p>支持基于 Web 2.0 的相关技术的应用系统检测；</p> <p>支持 HTML5、支持 WAP 协议；</p> <p>支持所有类型的静态和动态页面检测；</p> <p>支持 WAF 或其它防护工具的识别，能识别国内外常见 WAF 防护设备。</p> <p>4.3 可用性检测</p> <p>支持检测网站首页响应速度，支持检测域名劫持；支持获取网站信息；支持云端可用性。</p> <p>4.4 挂马检测</p> <p>支持网站挂马检测功能，每天自动更新源址库，云端动态行为检测技术与静态特征匹配相结合。</p> <p>支持识别挂马常见的加密算法、挂马代码模式。</p> <p>支持提供网站链接拓扑关系。</p> <p>支持取证存储功能，可配置留存所有页面或恶意页面。</p> <p>4.5 暗链检测</p> <p>基于云端暗链源址库，每天自动更新。</p> <p>4.6 变更检测</p> <p>可监测网站变更情况，并根据配置可减少对网页内容正常更新做出的报警。</p> <p>4.7 敏感内容检测</p> <p>对网站页面中的内容进行敏感内容（涉黄、涉毒、涉赌博、涉政治等敏感内容）检测。</p> <p>4.8 脆弱性检测</p> <p>SQL 注入检测功能，检测网站是否存在 SQL 注入漏洞；</p> <p>支持常见服务器脚本语言安全漏洞；</p> <p>支持 Web 路径下敏感文件检测；</p> <p>支持对常见的开源或收费第三方应用进行漏洞检测。</p> <p>4.9 支持深层次入侵式测试</p> <p>5. 域名探测</p> <p>支持站点资产自动发现能力，能够快速发现 IP 地址段内存活的 IP 地址及对应站点的属性信息</p> <p>6. 报表功能</p> <p>支持网站目录树结构展示，支持历史统计报表。</p> <p>7. 扫描性能</p> <p>单台设备每天的检测能力达到 100 万 URL 以上。</p> <p>8. 报警功能</p> <p>支持邮件告警，可灵活订阅告警邮箱及告警项目。</p> <p>9. 自动任务</p> <p>支持周期性检测，支持分钟级别的检测周期。支持各个模块设置不同检测周期。</p> <p>10. 扩展性</p> <p>支持基于认证授权的开放式 API 接口，能够通过接口实现任务下发，检测结果汇总；</p>

分项指标	技术参数、功能要求及具体配置
	支持与网络安全态势感知监测预警平台兼容对接；支持与上级主管单位重要信息系统及互联网网站远程执法检查平台系统的对接。 11. 升级性 不同时期规则库、软件版本应能向下兼容，易于升级；支持在线自动升级、离线升级。 12. 部署方式 支持多种部署方式：支持互联网（独立 IP 地址）直接部署模式；支持局域网环境部署模式。 13. 系统自身安全性要求 系统具有权限管理功能；支持日志审计功能；要求系统采用自行编译、经安全加固的 linux 操作系统；系统具备通过局域网部署模式实现大规模互联网业务监测能力。
监测数量	监测站点数量≥200 个
售后	1、硬件设备免费质保五年，硬盘无返还服务。 2、软件提供三年原厂商软件升级服务。

1-2 互联网域名安全巡管系统

分项指标	技术参数、功能要求及具体配置
系统基本要求	采用远程直接检测方式，对批量网站远程进行域名分析及被黑监测，判断网站信息变动情况，提供如下能力： 1、针对辖区网站底数进行智能分类判断，实时更新网站数量变更情况以及分布情况； 2、对重点网站域名使用情况进行综合管理； 3、针对最新网站域名清单进行最快分钟级网站首页被黑判断，确保网站安全事件由管理部门首先发现、先应急、快立案、早汇报的主动工作流程； 4、针对国内外反动势力及活跃黑客团体进行行为轨迹的跟踪与分析。 联动增强管辖区域内网站被黑监控能力。
物理特性	1U 机架式，处理器不低于 Intel Xeon E3 系列； 内存不低于 8GB，硬盘不低于 1TB SATA 。 接口：2 个 10/100/1000M 网络接口
关键点分析监测	1. 域名添加：支持单个或多个域名添加，支持系统自动判断子域名级别； 2 域名查询与删除 支持域名模糊查询，支持单位名称查询域名，支持 IP 地址范围查询域名； 域名列表可区分系统域名及发现域名，可显示域名备案信息、title 信息及域名状态（有效、无效）； 域名列表操作可支持详情查询、删除，可在域名列表中直接创建域名分析任务； 域名回收站； 支持模糊查询回收站中域名，支持单位名称查询域名。支持 IP 地址范围查询域名； 支持域名批量认领； 垃圾域名清理。 系统自动判断失效域名，支持失效批量域名清理。 3. 域名库导出

分项指标	技术参数、功能要求及具体配置
	<p>支持导出本地域名库，回收站与名表及清理域名表。 可支持导出 excel、csv 格式。</p> <p>4. 域名分析服务端 支持通过主域名自动分析该域名所有二级域名，支持域名行政归属判断； 可自动过滤泛解析域名，支持黑名单算法，支持基准对比去重。</p> <p>5. 监测任务设置 支持创建关键点监测任务，可设置监测地区，任务执行周期，支持标题页面内容检测，关键词设置。</p> <p>6. 任务管理 支持查询任务状态，执行总时间，已执行次数。可删除、修改已创建任务。 支持添加非本地域名库域名。</p> <p>7. 任务统计 支持基于时间轴的多维度数据统计； 支持分类别事件统计，支持饼图、梯形图、漏斗图自动切换，支持数据显示手动切换。</p> <p>8. 关键词管理 可管理关键词列表、支持批量删除关键词、支持分类别添加关键词、支持命中关键词频率统计。</p>
通知管理	<p>1. 通知列表：支持近期篡改事件，发现域名统计，支持域名篡改事件列表管理，可查询详情。</p> <p>2. 通知设置：支持多级别定义通知人员属性，通知任务列表批量管理，可分别设置域名发现事件通知及页面篡改事件通知。</p> <p>3. 支持邮件通知。</p>
信息展示	<p>1. 照片墙展示：支持展示本地、近期页面篡改事件照片墙展示，可查询详情，支持反共黑客篡改标识。</p> <p>2. 黑客动向：支持以新闻列表的形式，展现国内外黑客团体动向： 1) 支持云端监测获取的国内外黑客动向； 2) 支持监测反共黑客论坛自动检索，实时发现反共黑客论坛更新内容。</p> <p>3. 域名动态展示：支持分别统计近期发现域名及失效域名列表。 支持多图形展示域名统计信息。</p>
爬取及检测	<p>1. 规则要求 支持单个页面定制爬取规则. 通过针对某些网站定制的规则有效避免网站因为设计不符合规范而造成的自动爬取出现的错误； 单页面定制爬取规则可定制内容包括：检测的关键字，页面的编码，页面的标题，爬取的超时时间，爬取的类型等。 标题检测：支持多个有效标题的存储识别，有效降低误报率。 关键词检测：支持分词匹配，避免断句不当而产生误报。</p> <p>2. 爬取特性 支持爬取任务的实时监控，可显示具体任务的执行状态(完成度百分比)。 支持事件的聚合，在一定时间段内多任务重复检测到的问题页面不会重复报警。 支持网站页面多状态标识：支持正常状态、失败状态(某些网站已经关停不可访问)，</p>

分项指标	技术参数、功能要求及具体配置
	以及挂起状态(用于标明哪些网站出于维护或者限制访问)。 支持页面跳转检测,支持有效链接的存储,提升爬取性能和准确性。 系统支持 api 接口,支持基于 OAI(Open API Initiative)的 web 界面,提供了所测即所得的测试环境。 爬取网页代码支持高亮显示,方便篡改内容的查看与定位。
系统管理	系统升级:支持版本自动检测,支持在线、离线系统升级。
系统自身安全性要求	系统安全性:系统具有权限管理功能; 支持日志审计功能; 要求系统采用自行编译、经安全加固的 linux 操作系统; 系统具备通过局域网部署模式实现大规模互联网业务监测能力。
监测数量	监测站点数量≥200 个
售后	1、硬件设备免费质保五年,硬盘无返还服务。 2、软件提供三年原厂软件升级服务。

1-3 互联网边界安全监测分析系统

分项指标	技术参数、功能要求及具体配置
设备要求	1、平台可支持多种部署模式,包括虚拟化部署、硬件部署、软件部署、Docker 部署。 2、平台架构具备高可扩展型,可支持分布式部署方式,适应大规模部署,作为综合性平台,功能模块需独立,数据存储平台、控制引擎、扫描引擎。由控制引擎控制任务调度,下发任务给扫描引擎对目标进行扫描,完成扫描后,扫描引擎将数据存储到存储平台,通过展示平台进行展示,扫描引擎可随着扫描需求灵活添加,完成快速扩容。 3、设备特性: 2U 机架式 X86 架构加固定制国产服务器,处理器不低于 Intel Xeon E5 系列; 内存不低于 16GB,硬盘不低于 1TB SATA 6Gb; 接口:2 个 10/100/1000M 网络接口。
任务下发	平台可针对 IP,网段等类型数据自动开始扫描与监测任务。
资产探测与发现	1、使用反向域名解析,大数据等技术自动发现一级域名,并获取其对应的备案信息等数据。 2、子域名发现,可自动从一级域名出发,主动挖掘其发布在公网子域名。 3、端口与服务发现,平台可对目标进行 65535 全端口扫描,并识别整理出端口状态,开放的服务、使用的组件与应用类型及其版本等信息。 4、操作系统识别,根据发现的端口与服务,进行深度分析与检测,识别其操作系统。 5、Web 应用识别,平台可对 web 系统进行深度识别,包括其使用的开发语言、开发框架、Web 容器、页面标题等数据。
风险管理	1、漏洞验证,平台可对目标进行漏洞验证,包括常见资产系统漏洞、弱口令、SQL 注入、跨站脚本,扫描的所有结果均可提供漏洞的判断依据、漏洞来源,非通过版本方式进行判断; 2、开源社区监控,平台可根据用户自定义的关键字对 Github 社区的源代码进行

分项指标	技术参数、功能要求及具体配置
	监控； 3、敏感路径检测与持续监测，平台可针对 web 系统进行常见的敏感路径检测与持续监测，自动探测可能存在的漏洞与风险； 4、弱密码爆破，针对收集到的登录入口，可自动进行弱密码爆破。
安全情报	平台可通过多种渠道收集各种安全资讯（CVE 漏洞、freebuf、中国国家信息安全漏洞库等）、情报，收集最新最权威的漏洞信息，支持黑域名、黑 IP 情报数据。
数据接口	平台支持用户自主进行二次开发，用户可提供 API 接口读取数据，对数据进行二次加工。
售后	1、硬件设备免费质保五年，硬盘无返还服务。 2、软件提供三年原厂商软件升级服务。

1-4：教育互联网应用安全态势感知和通报预警平台（二期）

指标项	功能及技术参数要求
网络资产信息探测功能要求	1、Web 网站发现。可自动从 IP 地址段出发，主动探测和挖掘出属于该地址段的网站地址，并获取该网站相关的站点信息，包括网站标题、Web 容器、服务器信息等。 2、开放端口信息发现。可自动从给定的 IP 地址出发，探测属于该 IP 地址下开放的网络端口信息，并获取该端口下的网络服务类型，网络组件信息以及端口开放状态。 3、子域名发现。可自动从一级域名出发（如 test.com），主动挖掘其发布在公网子域名。ICP 备案发现、平台支持 ICP 备案自动识别；登录页面自动识别，平台可通过搜索引擎、页面数据自动识别主域名下的所有登录页面。
网络安全监控事件预警	1、域名巡管被黑监控，通过下发域名巡管监控任务，实现指定域名下网站被黑客篡改的事件预警，并且能够对被黑事件进行等级划分，提供网站被篡改详情信息，和网站被黑快照。 2、网站漏洞实时监控，通过下发网站漏洞监控任务，实现对网站漏洞的实时监控，包括网站可用性信息，网站的漏洞风险，并对网站安全风险划分等级，提供漏洞详情信息。 3、网站漏洞验证，通过下发网站漏洞验证任务，验证目标节点网站是否存在安全机构发布的公共漏洞，并提供漏洞详情和漏洞修复方法。 4、开源社区监控，如 Github，平台可根据用户自定义的关键词对开源社区的源代码进行数据采集和实时监控，获取所有与关键词相关的源代码段，自动识别代码语言并实现代码高亮。
网络安全漏洞信息采集与监控	漏洞社区监控，平台可根据用户提供的关键字，针对当前流行的漏洞社区进行监控，针对每项漏洞信息提供具体的解决方案。
网络安全态势数据可视化展示	1、区域安全态势总览。平台可以实现指定区域内所有目标节点安全态势统计和可视化展示； 2、区域安全通报统计。平台可以实现指点节点的安全预警通报统计和可视化展示，并对各个节点单位对事件的处理能力进行评估； 3、目标网络资产探测。平台可以实现指定区域内所有目标节点资产数据的统计和可视化展示。

指标项	功能及技术参数要求
目标资产信息管理	提供信息安全集中管理功能，包括：资产信息维护（如被监管单位信息基础信息管理、单位域名信息管理、单位网络信息管理等）、服务和工具管理（扫描任务管理、扫描工具和参数管理等）等功能。
安全预警及响应	1、数据采集管理：能够自动采集网站监测、域名巡管以及互联网安全态势探查平台的数据，并统一整合分析处理； 2、提供事件类数据的技术审核以及发布审核，并将数据内容通报至目标节点等功能； 3、提供快速定位事件、闭环处理事件的功能； 4、提供安全事件分类查询、统计，处理状态查询和统计等功能。 5、提供发生安全预警信息后，能够通过预设的条件尽快通知到相应负责人的功能。告警设置可以根据预警的对象，预警方式做设置，以便安全预警算能通过短信、邮件、登录提示等方式通知到相关负责人。
对接	△1、实现与教育互联网应用安全态势感知和通报预警平台（一期）无缝对接，对接内容包括： （1）一期平台可接入本期实施的 1-1、1-2、1-3 应用安全态势感知探针数据； （2）二期平台可接入一期已实施的网站安全监测 (websoc) 的态势感知探针数据。 2、提供制造厂商针对本项目授权书与制造厂商售后服务承诺函。
售后	1、硬件设备免费质保五年，硬盘无返还服务。 2、软件提供三年原厂商软件升级服务。

1-5 安全应急支撑服务

指标项	功能及技术参数要求
总体要求	针对用户系统的安全需求，为用户系统提供安全应急响应服务，对于突发的安全事件在最短时间内做到应急响应，了解安全事件的基本现象，判断安全事件的原因，进行故障和事件的处理，并针对安全事件形成的破坏做出灾难恢复，在必要的情况下，协助用户针对系统进行入侵追踪和犯罪取证。
服务内容	应急安全响应服务包含以下内容： 1、恶意入侵事件分析，病毒木马分析，恶意篡改事件分析，入侵追踪，犯罪取证，协助安全加固。 2、检查支撑：协助用户开展系统安全检查工作。 3、报告支撑：协助用户开展系统安全监测报告的梳理汇编工作。 4、重保支撑：协助用户在重要系统安保时期开展保障支撑工作。 5、案（事）件支撑：协助用户开展系统安全案（事）件的侦查、调查和取证工作。 6、通报预警支撑：协助用户开展管辖范围的系统安全态势、安全情报的通报预警工作。
服务要求	响应时间： 1、提供 7*24 小时应急响应服务。 2、如发生事件或异常，应急响应人员应在 15 分钟内予以响应。 3、如事件或异常需要紧急处理，应急响应人员需在 3 小时内赶赴现场。
服务期	1 年

项目 2：郑州教育管理公共服务数据安全防护

1、业务需求

随着信息技术与教育教学的深度融合发展，以数据库为基础的信息系统在郑州教育信息基础设施建设中得到了广泛的应用，越来越多的数据信息被应用于教育业务信息的搜集、存储以及发布，并在此基础上形成了行业合作和数据共享的教育数据中心。但是在新的网络环境中，由于信息的易获取性，这些包含在数据库系统中的关乎国家安全、个人隐私等涉密信息将面临更多的安全威胁。

现有边界防御安全产品和解决方案均采用被动防御技术，无法从根本上解决各组织数据库数据所面临的安全威胁和风险，解决数据库数据安全需要专用的数据库安全设备从根本上解决数据库安全问题，由此提出数据库安全防护项目，包括数据库防火墙和数据库安全服务。

2、产品需求一览表

序号	名称	单位	数量
2-1	数据库防火墙	台	2
2-2	数据库安全运维服务	年	1

3、技术参数

(2-1) 数据库防火墙

指标项	功能及技术参数要求	
规格指标	硬件设备	标准的 2U 硬件设备，双电源； 硬盘不低于 3T，可支持 RAID0\RAID1\RAID5 存储； ≥1 个 100/1000 Base-Tx 管理口； ≥1 个 HA 接口，可切换为管理口； 板载 ≥4 个 100/1000M 电口，支持 2 组透明网桥直联串接（bypass）模式；
	性能	支持 10000 条 SQL/秒级吞吐量； 支持 3000 条并发链接；
	数据库类型	1、支持国际主流数据库：Oracle（含 Oracle 12C）、SQL Server（含 SQL Server 2014）、MySQL、DB2、Postgres、sybase 等； 2、支持国产数据库：达梦(DM)、南大通用(含 GBase8T)、人大金仓(KingBase)、神通(Oscar)等。
防护规则	控制模式	中断会话：对需要阻断的访问，中断数据库连接 拦截语句：对需要阻断的访问，返回防火墙的错误提示信息，当前语句被拦截后，该会话不中断。
	行数阈值管控(投标时提供厂商盖章的产品截图)	针对数据库数据表，可按照受影响数据行数(阈值)进行精细管控，超出阈值的行为进行阻断或拦截，防止高危操作或大批量数据泄露。
	加密账户规则	支持 SQL server 2005 以上(含)版本，对加密数据库用户名的解析；支持数据库账户的防护规则设置；
	防护规则元素	1、客户端信息：客户端 IP、数据库用户、客户端工具、MAC 地址、操作系统用户、主机名； 2、应用信息：应用客户端 IP、应用账户；

指标项	功能及技术参数要求	
		3、操作类型：DML、DDL、DCL； 4、对象：数据库、schema、表、字段； 5、执行结果：影响行数、响应时间、结果关键字、应答错误号； 6、other：关联表个数、关键字等
	策略管理	1、支持全局策略设置，基于全局策略可以下发给每个数据库设置规则； 2、支持策略的导入、导出设置； 3、支持单项策略的状态管理，手动完成修改、开启和关闭等操作； 4、支持基于多条规则的逻辑关联，根据排列区分优先级； 5、支持语句管理，增加例外规则完善策略； 6、支持默认规则组，针对不同数据库提供默认规则
	△防护规则设置 （投标时提供厂商盖章的产品截图）	对以下高危行为，可自动识别并进行安全防护和告警通知： 1、批量数据导出：对超过特定行数阈值的批量数据导出行为； 2、高危操作：对超过特定行数阈值的批量数据修改、删除； 3、支持 no where 全表 Update、Delete 行为防护； 4、支持口令攻击防护，可基于频次判断失败登录风险； 5、支持关联表个数设置； 6、支持返回错误码； 7、支持应用关联防护策略； 8、支持周期内频次行为防护； 9、提供自定义扩展规则，实现灵活的规则设置； 10、支持 SQL 语句模板化归类，基于语句模板关联客户端信息自定义风险语句
	敏感数据防护	支持数据库字段级的与或逻辑设置，可建立敏感数据组进行专项安全防护
应用防护	应用关联防护	1、采用应用端轻量级插件部署，以精确方式审计到应用端相关信息， 2、支持应用账号和应用 IP 的关联解析，并基于应用信息设置防护规则； 3、支持 Weblogic、tomcat、Websphere、Jboss 等主流的应用服务器； 4、支持对 F5 等负载均衡模式下虚拟 IP 的识别，深入挖掘原始应用 IP； 5、支持 Apache HttpClient 和 JDK1.6 JAXWS 环境下的四层关联审计解析；
	数据库漏洞攻击防护（投标时提供厂商盖章的产品截图）	1、提供利用 CVE 上已公开的数据库漏洞，进行攻击拦截的虚拟补丁； 2、漏洞分类涵盖：缓冲区溢出、权限提升、拒绝服务攻击等； 3、提供 400 个以上虚拟补丁； 4、支持对绿盟 RSAS 等国内主流漏洞检测工具的扫描防御；
	SQL 注入监测	1、支持 SQL 注入、XSS 攻击等外部行为防护； 2、支持根据 IP、sql 特征自定义 SQL 注入规则； 3、支持 SQL 注入例外规则设置；
运维审批及管控	△运维申请 SQL 语句申请方式（投标	1、运维人员以完整 SQL 语句形式提交申请，选择对应审批人，并根据操作时间指定本人执行或授权其他人员； 2、在提交语句申请时，可选择是按照完整语句审批，或按照语句模板

指标项	功能及技术参数要求	
	时提供厂商盖章的产品截图)	(不含参数) 审批;
	运维申请—脚本申请方式	运维人员可以上传脚本文件至系统中申请, 系统支持多个脚本文件上传申请;
	运维申请-组合条件申请方式	按照“客户端工具+地点(IP)+时间+对象(表、函数、存储过程等名称)+操作(DDL、DML、DCL等)”的条件组合提交申请。
	多级审批	系统可以设置多级审批, 提高运维审批强度、规范运维流程
审计分析	审计内容	<ul style="list-style-type: none"> 1、会话的终端信息: IP、MAC、Port、工具名称(程序名)、操作系统用户; 2、会话的主机信息、IP、Port、数据库名(实例名)、业务主机群; 3、会话的其它信息: 登录时间、会话时长; 4、操作信息: 操作类型(DDL、DML、DCL等)、操作时间、执行时长、SQL语句、操作对象(数据库实例、schema、表、字段、函数、存储过程名称)、SQL错误代码; 5、操作影响范围信息: 查询、修改、删除操作的影响行数, 以及返回行数; 6、支持数据库双向审计; 7、支持结果集审计、记录操作成功与失败; 8、支持对超长SQL操作语句解析, 单条语句长度可达2M;
	审计查询	<ul style="list-style-type: none"> 1、支持基于时间、IP地址、数据库服务器IP地址、用户名、数据库操作命令、数据库表名, 执行结果, 应用用户等多种丰富的查询检索条件; 2、支持应用层关联审计查询和关联分析;
	风险分析	<ul style="list-style-type: none"> 1、支持风险统计: 统计全局和单库的风险命中情况; 2、支持风险源分析: 基于客户端IP、数据库用户、工具和应用分析风险来源;
	检索分析	支持风险、语句、会话等多维度的详情检索能力;
	告警审计	对满足一定风险级别的访问行为记录到告警表中, 快速提供给用户进行实时监控和查询;
	告警策略设置	<ul style="list-style-type: none"> 1、支持高、中、低风险告警, 2、支持风险登陆、风险操作、SQL注入、漏洞攻击检测、口令攻击、频次攻击等中风险告警; 3、支持系统资源监控与告警。
	告警方式	<ul style="list-style-type: none"> 1、告警方式包括: 邮件、短信、SYSLOG、SNMP、界面; 2、支持短信平台对接, 发起告警操作;
	备份和恢复	<ul style="list-style-type: none"> 1、支持审计数据自动备份到本地和远端FTP、SFTP、NFS服务器, 2、支持系统配置的导入导出; 3、针对不同的业务压力提供适用性备份方式;

指标项	功能及技术参数要求	
		高压压缩比存储：提供 10:1 的高压缩比，存储海量数据； 高性能存储：针对实时压力较大，需要快速备份存储的场景；
系统管理	IP 别名管理	支持客户端 IP 别名设置，针对不同客户端 IP 自定义别名展现；
	分组管理	支持数据库、DB 用户、IP、时间、对象、应用用户等多维度的分组管理。
	角色管理	支持建立系统账户角色，并根据角色分配产品功能使用权限；
	自身安全	根据三权分立的原则，提供系统管理员、安全管理员和审计管理员不同的用户身份验证。系统针对产品操作人员的操作行为进行审计记录，可以由审计管理员进行查询，具有自身安全审计功能。提供审计数据管理功能，能够实现对审计数据的自动备份、导入。
增强功能	管理界面要求	中文界面，B/S 架构
	学习建模	1、提供学习期并基于学习期完成语句、会话、行为建模，构建数据库安全防护模型。可抽象描述不同类型的 SQL 语句，规避参数带来的多样化；2、并通过学习期捕获全量的 SQL 语法，归类形成 SQL 语句模板，用户可建立信任语句规则对合法的 SQL 模板默认放行。
	协议解析	1、支持协议自动识别数据库信息； 2、支持无链接会话识别； 3、支持 Oracle、SQLserver 动态端口下的解析
	自动诊断	支持产品自动诊断能力，可针对产品的引擎、策略中心等区域提供自动诊断报告，便于产品异常排查和维护；
网络部署	网口自识别	支持监听端口自动识别，无需网口配置即插即用； 支持管理口速率自动协商；
	△网桥模式	在网络上物理串联接入数据库防火墙设备，所有用户访问的网络流量都串联流经设备，通过透明网桥技术，客户端看到的数据库地址不变。
	代理模式	1、网络上并联接入数据库防火墙设备，客户端逻辑连接防火墙设备地址，防火墙设备转发流量到数据库服务； 2、可支持主备模式部署；
	旁路模式	在旁路部署模式下，通过 TAP、SPAN 等技术将网络流量映射到审计设备，对数据库流量进行审计和告警；
	HA 主备模式	支持 HA 双机主备自动切换，支持策略同步、会话同步机制，保障多设备间的一致性；
	负载均衡模式	支持 F5 等负载均衡器，采用防火墙代理模式部署，支持负载均衡下的链路检测与切换
	支持 bypass 容灾	支持产品断电 bypass 和在线 bypass 容灾功能，可自动启动和关闭网口间 bypass 导通，保障系统异常环境下的网络畅通； 支持手动 bypass 功能，在应急情况下，可手动导通网络避免异常阻断。
	支持多 VLAN	支持当交换机产生多 VLAN（虚拟局域网）时对数据库防护能力

指标项	功能及技术参数要求	
	支持跨网段访问	支持网络环境中跨网段访问数据库的安全防护能力
产品资质要求		1、提供国家版权中心颁发的软件著作权； △2、提供在“公安部官网”可查询，具有公安部颁发在有效期内的“计算机信息系统安全专用产品销售许可证”。
服务		1、提供应急预案、提供备机。 2、按需求定制报警策略、提供同行业或其他行业策略定制参考。 3、协助分析核心应用系统数据库的关键表、字段等需要防护的内容，并根据内容指定报警策略。 4、解决数据库防火墙报警事件，解决安全事件。 5、协助分析安全事件，协助分析及加固数据库安全防范。 6、报警结果处理、解决报警事故、提供书面解决过程。 7、提供1月一次巡检服务； 8、硬件设备免费质保五年，提供硬盘无返还服务；软件提供三年原厂商软件升级服务；数据库漏洞攻击特征库提供三年免费升级。 9、提供制造厂商针对本项目授权书与制造厂商售后服务承诺函。

(2-2) 数据库安全运维服务

指标项	内容及要求	
数据库安全服务	数据库安全风险评估服务	从数据库系统、操作系统、管理制度、管理员等多个角度进行全面的数据库安全风险评估服务，发现潜在的数据安全威胁及隐患。
	数据库安全防护服务	针对 SQL 注入和数据库漏洞攻击行为进行整体防护，采用主动防御的技术及时拦截风险行为并提供报警： 1、数据库主动防护规则配置服务； 2、主动防护策略管理服务； 3、数据库漏洞虚拟补丁防护服务 4、应用关联防护服务； 5、分析行为审计服务； 6、风险行为分析服务； 7、风险行为告警服务； 8、访问行为黑白名单建立服务
	数据库安全运维服务	面向数据库运维人员，针对数据库系统日常运维管理工作，能够有效提升精细度及安全性 1、数据库运维操作控制服务； 2、数据库运维细粒度权限管理服务； 3、运维行为审计服务； 4、数据库运维申请审核流程制定服务； 5、数据库运维风险行为风险告警服务。
	数据库漏洞扫描服务	1、针对用户现有数据库进行漏洞扫描服务并提供修复建议。漏洞扫描范围包括：权限风险、配置风险、弱口令风险、数据库漏洞等。 2、检查数据源中的 PCI DSS、PII、SSN、HIPPA 等敏感数据并进行分类

指标项	内容及要求
	<p>3、使用预先配置的漏洞测试，包括 Center for Internet Security (CIS) 和 Security Technical Implementation Guide (STIG)。</p> <p>4、提供特定于平台的静态测试，检测正在评估的特定数据库的不安全配置。</p> <p>5、执行动态测试以发现行为漏洞，例如，帐户共享、登录失败次数过多和不正常的非工作时间活动。</p> <p>6、检测影响系统可用性的入侵式利用或测试，并提供外部引用信息，例如，公共漏洞和暴露 (CVE) 标识</p> <p>7、对发现的数据库漏洞提供详细的扫描报告及相应的修复建议。</p>
△数据库渗透验证服务	<p>1. 提供模拟黑客式的检查手段，通过模拟黑客攻击的方式，利用数据库本身存在的漏洞，获取数据库管理员的权限并登录到数据库，实现直接取证。</p> <p>2. 攻击方式： SQL 注入渗透：利用 SQL 注入漏洞进行权限提升；缓冲区溢出攻击：利用缓冲区溢出的方式，造成数据库服务崩溃，实现拒绝服务攻击。</p> <p>3、数据库渗透测试服务。</p> <p>4、数据库渗透测试策略配置服务。</p> <p>5、数据库渗漏测试报告服务。</p>
数据库账号整理及权限梳理服务	<p>1、帮助用户发现、整理其环境中的数据库账号，并对数据库账号进行权限梳理。</p> <p>2、为用户调整账号权限，调整防御策略提供数据支撑。</p> <p>3、进行数据资产权限变更梳理，登记数据库中过期用户数据权限登记，登记活跃用户权限使用情况。</p>
数据库安全产品策略定制服务	<p>1、对数据库安全产品提供策略定制服务，根据用户实际情况，针对性的制定防御策略，帮助用户将产品的功能效果最大化。</p> <p>2、实时执行安全策略，监控并实施安全策略，及时发现敏感非结构化数据访问、特权用户操作和变更控制。</p> <p>3、使用访问策略来发现异常行为，例如大批量更新和删除数据，导出数据行为进行控制，支持基于策略的操作，例如审计、接近实时的安全警报和阻断操作行为等。</p>
△数据库行为审计服务	<p>1、监控和审计所有数据活动，了解并全面洞察由用户、开发人员、外包人员和应用对文件系统、固定存储器和移动存储器执行的所有操作。发现尝试进行未经授权访问的用户。</p> <p>2、操作系统日志记录和审计功能的用户和应用访问监控功能。通过检测不正常的文件和文档读写活动，提高数据安全性。</p> <p>3、将所有文件和元数据归档，清晰地掌握非结构化数据的全貌。</p> <p>4、创建集中的审计数据存储库，汇集整个企业的数据库，进行合规审计和报告、关联及取证。</p> <p>5、定制的合规工作流程，用于生成合规报告，并将报告分发给监督团队以进行电子会签和上报。</p>
数据库安全培训服务	<p>通过分析数据库自身安全缺陷、B/S 架构下的数据库安全风险、复杂运维环境下的数据库风险、数据库安全攻防演练，提高客户方的数据库安全整体意识，对于数据库安全的常见风险、主流技术手段有深入</p>

指标项	内容及要求	
		的了解。
	数据安全应急响应服务	1、针对信息系统中的数据、制定应急响应预案，并有计划的进行演练和改进； 2、针对信息系统突发的重大安全事件，以最快的时间进行故障排查定位和应急处理。
	驻场运维	1 名驻场数据库工程师提供 5*8 小时按现场实际工作需要提供值班及备勤服务。
服务期限	1 年。	

项目 3：郑州教育数据中心重要信息系统安全服务项目

1、项目背景

为认真贯彻和落实中央 27 号文件《国家信息化领导小组关于加强信息安全保障工作的意见》、《河南省人民政府办公厅关于印发 2012 年河南省信息化建设专项方案的通知》、《关于印发河南省关键基础设施网络安全检查工作方案》的通知（豫网办发[2016]18 号）、《中华人民共和国网络安全法》等文件要求，切实提高信息系统安全保护能力和信息安全管理水平，将按照国家相关要求开展信息安全等级保护测评工作。

依据《信息安全等级保护管理办法》（公通字[2007]43 号）、《信息安全等级保护基本要求》、《信息系统安全等级保护实施指南》（信安字[2007]10 号）、《信息安全等级保护安全建设整改工作指导意见》（公信安[2009]1429 号）等相关文件要求，为全面提升信息系统的安全保障能力和防护水平，对信息系统进行全面的安全等级保护测评工作，并提供安全建设整改意见中除设备采购外的安全整改服务。

2、项目范围

按照等级保护的相关标准进行等级保护安全测评工作，对郑州市教育局电化教育馆负责维护管理的郑州教育管理云平台、郑州教育信息网、郑州教育云数据中心、郑州教育公共服务平台等系统发现可能存在的问题，出具信息系统安全保护等级测评报告，协助完成信息系统安全保护等级备案工作，并取得定级备案证明。

3.1 等级测评要求

3.1.1 测评内容

本项目按照信息安全等级保护的安全等级测评标准进行安全等级测评，等级测评的现场实施过程由单元测试和整体测评两部分构成。

对应《基本要求》各安全控制点的测评称为单元测试，具体可分为物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统

运维管理十项测试任务。

整体测评是在单元测评的基础上，通过进一步的分析信息系统安全保护功能的整体相关性，对信息系统实施的综合安全测评。

测评的内容包括但不限于以下内容：

安全技术测评：包括物理安全、网络安全、主机系统安全、应用安全和数据安全等五个方面的安全测评；

安全管理测评：安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全测评。

（1）物理安全

根据系统机房和现场安全测评记录，针对机房和现场在“物理位置选择”、“物理访问控制”、“防盗窃和防破坏”、“防雷击”、“防火”、“防水和防潮”、“防静电”、“温湿度控制”、“电力供应”和“电磁防护”等物理安全方面所采取的措施进行，判断出与其相对应的各测评项的测评结果。

（2）网络安全

根据系统网络安全测评记录，针对网络方面在“结构安全”、“访问控制”、“安全审计”、“边界完整性检查”、“入侵防范”、“恶意代码防范”、“网络设备防护”等网络安全方面所采取的措施进行检查，判断出与其相对应的各测评项的测评结果。

（3）主机安全

主机安全现场测评包括对系统服务器的测评，测评内容包括“身份鉴别”、“访问控制”、“安全审计”、“剩余信息保护”、“入侵防护”、“恶意代码防护”、“资源控制”。

（4）应用安全

应用安全现场测评包括对系统测评，测评内容包括“身份鉴别”、“访问控制”、“安全审计”、“剩余信息保护”、“通信完整性”、“通信保密性”、“抗抵赖”、“软件容错”、“资源控制”方面。

（5）数据安全及备份恢复

系统数据安全及备份恢复现场测评包括“数据完整性”、“数据保密性”、“备份和恢复”几个方面的测评。

（6）安全管理制度

根据现场安全测评记录，针对系统系统在安全管理制度方面的“管理制度”、“制定和发布”以及“评审和修订”等测评指标，判断出与其相对应的各测评项的测评结果。

（7）安全管理机构

根据现场安全测评记录，针对系统在安全管理机构方面的“岗位设置”、“人员配备”、“授权和审批”、

“沟通和合作”以及“审核和检查”等测评指标，判断出与其相对应的各测评项的测评结果。

(8) 人员安全管理

根据现场安全测评记录，针对系统在人员安全管理方面的“人员录用”、“人员离岗”、“人员考核”、“安全意识教育和培训”以及“外部人员访问管理”等测评指标，判断出与其相对应的各测评项的测评结果。

(9) 系统建设管理

根据现场安全测评记录，针对系统在系统建设管理方面的“系统定级”、“安全方案设计”、“产品采购和使用”、“自行软件开发”、“外包软件开发”、“工程实施”、“测试验收”、“系统交付”、“系统备案”、“等级测评”以及“安全服务商选择”等测评指标，判断出与其相对应的各测评项的测评结果。

(10) 系统运维管理

根据现场安全测评记录，针对系统在系统运维管理方面的“环境管理”、“资产管理”、“介质管理”、“设备管理”、“网络安全管理”、“系统安全管理”、“恶意代码防范管理”、“密码管理”、“变更管理”、“备份与恢复管理”、“安全事件处置”以及“应急预案管理”等测评指标，判断出与其相对应的各测评项的测评结果。

3.1.2 测评要求

在安全等级测评过程中，每个工作阶段、流程、内容及成果交付严格遵循《信息安全技术信息系统安全等级保护测评要求》和《信息安全技术信息系统安全等级保护测评过程指南》文件，根据信息系统安全等级，开展相应级别的安全等级测评工作，根据测评结果出具相应的单项和整体测评报告。测评报告编制的内容及格式严格遵照《信息系统安全等级测评报告模版（2015年版）》进行。

3.1.3 测评过程文档

项目各阶段的测评过程文档（参照《信息安全技术信息系统安全等级保护测评过程指南》）编制。

项目阶段	交付成果
测评准备活动	项目计划书 被测系统基本情况表
方案编制活动	测评指导书 信息系统安全测评方案
现场测评活动	测评结果记录 测评中发现的问题汇总
分析与报告编制活动	单项测评结果汇总分析 整体测评结果汇总分析 等级测评结论 信息系统安全等级测评报告

△3.2 测评生成物

通过现场测评，按照平台现有信息系统的情况，生成等级保护测评报告，对符合性进行评估后，提

供安全建设加固建议、安全检查测试，具体如下：

3.2.1 整改建议

依照《信息安全等级保护安全建设整改工作指导意见》（公信安[2009]1429号），严格遵循《信息安全等级保护安全建设整改工作指南》各项要求，在系统测评工作的基础上，对信息系统总体信息安全管理和技术方面现状进行全面的分析，制订信息安全等级保护安全建设整改建议方案，方案内容包含但不限于：信息安全背景、政策与技术标准依据、当前风险分析、安全需求分析、总体安全策略、安全建设整改技术方案设计、安全建设整改管理体系设计、信息系统安全产品选型及技术指标建议、安全建设整改项目实施计划、项目预算、整改后可能存在的其他问题。

3.2.2 项目交付成果

- (1) 《信息安全等级测评报告》
- (2) 公安部门颁发的《信息安全等级备案证明》

3.3 安全建设整改服务

能够根据安全威胁及时调整安全策略，从而提高信息系统的整体防御能力，实现对重要信息系统的重点保护；

建立符合当前安全需求的安全技术体系和安全管理体系，建立信息安全等级保护的长效工作机制。

整改服务完成时间要求：提交《信息安全等级保护安全建设整改建议报告》后 30 天内。

项目 4：郑州市市直学校网站安全监测项目

1. 建设目标

建设网站监测平台，为网站提供健康诊断和监控检测服务，提供深度的数据挖掘。通过对网站可用性监测、网站性能监测、网站敏感词监测、网站断错链监测、网站安全监测等手段，实现以下目标：

1. 实现对郑州市市直学校网站的日常监测，通过 7*24 小时的机器加人工服务，确保网站信息内容的安全和正常运维。
2. 为郑州市市直学校网站提供 7*24 小时断链、错链诊断，对网站运行状态进行监控，及时发现错误并改正。
3. 为郑州市市直学校网站提供敏感词汇检测功能，保障网站信息发布的准确性。
4. 为郑州市市直学校网站提供全面的运维监测服务，包括按栏目监测无效地址、各类应用服务监控和短信报警、安全监测等。

2. 技术参数

利用专业的网站监测平台，高频度扫描网站群网页，实现特征检查和内容检查，如果网页发生异常变化，则平台会发送短消息、邮件等告警信息。

针对防火墙软件的缺陷、以及网页防篡改系统对 SQL 注入攻击和路由攻击等的无能为力，利用专业的“网站安全监测值班中心”，采用“人+软件+告警通知”的模式，以“第一时间发现，第一时间阻断”为安全策略，实行 24 小时节假日不休的值班制度，为网站提供安全监测值班服务。

主要功能应包括：黑客挂马扫描；网站黑客自动监测功能；网站首页可用性、链接可用性监测；网页文件大小突变诊断告警；网站非工作时间文件上传扫描；网站敏感词汇扫描；网站栏目更新提醒。

利用以上方式有效地、最大限度的监测网页的安全性和网站可用性。

具体功能如下：

1. 网站性能模块功能

记录并统计网站首页的速度指标，绘制出该网页性能的历史趋势，协助网站管理员把握网站的总体性能变化趋势。提供：

监测网站的传输速度、响应时间、打开时间情况，并自动生成排名报表。

网站速度性能曲线，包括周曲线、月曲线

支持性能历史趋势分析，提供任意时间段的变化曲线

网站响应时间曲线对比

网站群性能排名报表，支持按传输速度、响应时间、打开时间排名

设置访问速度告警阈值，超过阈值自动进行短信告警。

2. 网站错误链接监测模块功能要求

对目标网站每一个动静态网页进行检测，并自动分析出这些网页的链接关系，根据分析结果判断网站是否存在缺页或者缺图的情况，或存在多媒体附件缺失的情况。

准确定位并跟踪网站错链

提供追踪功能，记录从首页到出错页面的路径，以便于迅速修复。

实时刷新故障列表，如原有错链断链被修复，则应对故障列表进行刷新以反映修复情况。

支持对某条错误的修复情况进行分析

支持对 JavaScript 形式链接的自动扫描，并支持多国语言的错误链接扫描和定位。

可按错误类型分类显示结果。

按栏目分类显示网站错误，支持树状显示方式，能够层层展开显示。

支持站内站外分类显示错误链接。

支持按照网站错误存在时间进行排列。

3. 网站安全监测模块

此模块是指以网页特征扫描为主要手段的被动式安全监控模式，应实现以下功能：

支持网站挂马监测与报警

可对网页敏感词监测

对非工作时间更新监测

对过大的图片进行监测

4. 功能指标

指标项	功能及技术参数要求
硬件环境	双核或双核以上 CPU，16G 以上内存，至少 1T 硬盘空间。
部署方式	1、支持旁路部署，无需改变原有的网络架构； 2、分布式部署。
功能要求	1、产品要求界面友好，并有详尽的技术支持文档，所有图形界面要求中文。 2、系统为 B/S 架构，并采用 SSL 加密通信方式，用户可以通过浏览器远程方便对产品访问操作，支持多用户同时登录操作。 3、提供分布式部署，上级管理设备能够方便查看下级设备状态。 4、提供三权分立的账户体系，支持上下级部门管理，非上下级的不同部门任务、资产隔离。 5、提供审计功能，能够对登录日志、操作日常进行记录和查询，并可以将日志导入导出操作。 6、提供日志自动审计功能，根据指定的审计标准自动、定时审计；并将审计结果发送到指定邮箱当中。
监测策略	1、支持漏洞扫描、网马监测、篡改监测、敏感关键字监测、可用性监测的独立策略设置，可独立配置监测周期、监测深度、监测页面数、监测引擎的独立指定； 2、平台支持策略的灵活配置，可配置网站中扫描页面黑白名单，爬行名单等，可支持在权限较高的管理后台中监测； 3、可限制扫描引擎的最大并发连接数，防止对网站产生过大访问压力； 4、平台提供多套策略模版与自定义策略模版管理功能； 5、平台支持任务模版的设定与调用； 6、平台支持在指定扫描时段的扫描，非允许时段会自动暂停扫描任务。
漏洞扫描	1、平台提供网页漏洞扫描，可扫描 SQL 注入、XSS 跨站脚本、伪造跨站点请求（CSRF）、网页木马、隐藏字段、表单绕过、AJAX 注入、弱配置、敏感信息泄漏、弱口令、Xpath 注入、LDAP 注入、框架注入、操作系统命令注入、Flash 源代码泄漏、Flash 跨域攻击、Cookie 注入、敏感文件、第三方软件、其他各类 CGI 漏洞等各种类型； 2、平台提供漏洞风险跟踪视图，进行历史风险跟踪与比对； 3、平台支持提供漏洞的风险分类视图、URL 树形结构视图以及网站结构图； 4、平台支持对注入类漏洞进行渗透功能，能实现提取数据库类型、名称、表与字段等数据； 5、平台支持对漏洞进行自定义检测功能，可修改测试请求再次检测； 6、平台支持对漏洞检测过程展现与分析，可比对正常请求与检测攻击的区别； 7、产品提供 Web 应用漏洞扫描功能，支持对 Discuz、大汉 CMS、PHPCMS、DEDECMS、ECSHOP、WordPress、eWebEditor、FCKeditor、Struts2 等国内外常见第三方组件扫描； 8、能够检测 GET、POST、User-Agent、Cookie 等多种方式提交的 HTTP 请求参数，并进行相应检测； 9、能够通过 Cookie 的方式支持对带验证码的应用系统进行扫描； 10、存在误报漏洞可通过产品在扫描结果处一键反馈给厂商协助修改； 11、支持识别国内外主流 Web 应用防火墙品牌； 12、支持识别被扫描目标对象的网站响应状态，能根据不同的响应状态直观呈现不同颜

指标项	功能及技术参数要求
	色标识。 7、管理人员可根据系统给出的漏洞参数、HTTP 请求/响应数据，快速验证，一键验证漏洞。
可用性监测	1、支持对网站的应用可用性监测，访问延时监测，能及时识别网站的应用异常； 2、支持按分钟设置监测频率 3、支持网站状态码展示，可以直观查看网站可用状态 4、支持 DNS 状态监测
关键词监测	1、支持按小时、天的时间设置监测频率； 2、支持查看关键词快照； 3、支持关键词检索，能快速查询存在关键词的网站。
变更监测	1、支持按小时、天的时间设置监测频率 2、支持首页变更监测，支持网站黑页监测，支持对网站源码比较
报告报表	1、提供风险值，1~100 内用于判断网站安全程度； 2、可进行各类风险纵向对比，实现风险跟踪，风险跟踪内容比对包括：新发现漏洞、已有漏洞、已整改漏洞； 3、可依据不同用户视角提供不同报告，如：管理者报告：提供漏洞分布统计信息，漏洞列表信息等；开发者报告：提供详细的漏洞测试方法，有隐患的参数等； 4、提供漏洞详细的整改建议； 5、能够提供多种统计分析报表，分析批量网站的漏洞等级与类型分布情况、排名情况、历史漏洞走势、各单位平均风险指数估计等。
即时告警	可提供灵活的告警阈值配置，包括依据风险等级告警，如中危以上弱点发送告警，高危弱点告警、任务结束告警等灵活配置；可限制每日告警次数上限，以免产生过多告警；对可用性告警，可配置异常时间阈值触发告警；可配置告警上限，限制告警次数；可定时发送网站安全监测的日报、周报、月报。
引擎调度	1、可实现引擎智能调度，可将任务负载均衡分配至饱和度较低的引擎； 2、任务下发前调用引擎进行扫描目标访问速度确认，择优下发至负荷小且速度快的引擎。
服务支持	1、提供 24 小时支持热线； 2、软件安装调试时，提供原厂产品培训服务； 3、一般故障处理响应时间≤4 小时； 4、本地应急响应时间≤2 小时。 5、硬件设备免费质保五年，提供硬盘无返还服务；软件及各类特征库提供三年免费升级服务。

说明：

(1) 投标文件中对某项技术指标如需更详细的表述，可单项另作文件说明。

(2) 招标文件中技术要求部分为满足采购人所需的最低要求，如有与某产品的指标或参数描述相同，并非特指，仅为招标货物质量、档次、水平的参照，评标以功能和性能为主。允许投标人以不低于招标文件要求的档次、技术、性能的软件产品参与投标。

(3) 安装、调试、检测、验收及标准等根据不同项目情况可另作详细的文字说明。

附件

评标标准和评标方法

一 评标原则

1. 公平、公正、科学合理评标；
2. 评标委员会由招标采购单位从政府采购专家库中随机抽取后并依法组建，有关人员对所聘任的评标委员会成员名单必须严格保密，与投标有利害关系的人员不得进入评标委员会；
3. 参加评标的人员应严格遵守国家有关保密的法律、法规和规定，并接受有关部门的监督；
4. 根据法律法规规定，参加评标有关人员应对整个评标、定标过程保密，不得泄露；
5. 评标委员会成员（以下简称评委）应按规定的程序评标；
6. 评委在开始评标前，应首先检查每份投标文件的内容是否完整，是否实质上响应招标文件的要求。对于实质上未响应招标文件规定的投标文件，采购人将予以拒绝。对于报价特别异常的，由评委依法认定。
7. 评标委员会将对确定为实质上响应招标文件要求的投标文件进行比较评审。
8. 投标人对评委施加影响的任何行为，都将被取消中标资格。

二 评标程序

1. 资格审查。开标结束后，首先按照《政府采购货物和服务招标投标管理办法》（财政部第 87 号令）由采购人对投标人的资格性进行审查。
2. 评标委员会根据评标原则和评标标准对所有资格审查合格的投标人的投标文件进行符合性审查，以确定是否满足招标文件的实质性要求。符合招标文件实质性要求的投标文件，评委将按评分标准进行价格评议和综合评分。

三 评分标准：

评分标准

（一）报价部分（30 分）

$$S_n = (C_{\min}/C_n) \times 30$$

S_n ：第 n 个投标人的价格得分

C_{\min} ：技术和商务初审符合的所有投标人的最低价格

C_n ：第 n 个技术和商务初审符合的投标人的投标报价

（二）商务部分（25 分）

1. 投标人业绩：8 分

（1）提供 2014 年 1 月 1 日（以合同签订日期为准）以来本单位已履行的信息化项目单个合同金额 300 万以上（含 300 万）的，包含合同和验收报告（或最终用户出具的证明材料），每提供一个得 2 分，最多得 8 分。

评标时验证原件，投标文件正本中提供复印件的并加盖公章，原件与复印件不一致的不予认可。

2. 质量保障：15 分

- (1) 投标人具有质量管理体系认证的得 1 分；
- (2) 投标人具有信息安全管理体认证的得 2 分；
- (3) 投标人具有信息技术服务管理体系认证的得 3 分；
- (4) 投标人具有国家保密行政管理部门授予的有效的《涉密信息系统集成资质证书》（甲级、乙级或单项）的得 3 分；
- (5) 投标人具有高新技术企业认证的得 3 分；
- (6) 技术力量保障情况 3 分。

依据投标人提供的参与本项目主要负责人和技术人员情况打分。依据与投标人签订的劳动合同和近一年来社会保险缴纳证明（在社会保险局官网上打印出的“基本养老保险个人权益记录单”为准。该材料附投标文件中），10 人以上的（含 10 人）得 3 分，否则不得分。

3. 售后服务：2 分

根据投标供应商承诺的运维服务，制定的组织结构、项目经理及人员构成、服务计划、人员培训、售后服务人员配备方案进行评比打分（0-2 分）。

（三）技术部分（45 分）

1. 投标产品技术指标响应程度（12 分）

招标文件中标记*的技术指标投标人所投标产品如果有不满足的不予以接受；带△的技术指标每有一项不满足的扣 1 分；其余指标项由于技术原因达不到招标文件要求的，每有一项不能满足的扣 0.5 分，扣完为止。

2. 生产厂家综合实力（8 分）

项目 1：教育应用安全态势感知平台项目生产厂商为公安部开展重要信息系统和政府网站安全专项检查工作的授权合作单位（提供公安部授权文件复印件加盖厂商公章）、国家互联网应急中心网络安全应急服务支撑单位的得 3 分，没有不得分。

项目 2：郑州教育管理公共服务数据安全防护项目所投“数据库防火墙”生产厂商具备数据库漏洞挖掘能力，提供已挖掘且得到 CVE 和 CNNVD 确认的数据库危险漏洞，至少具备国外和国内的数据库漏洞各 2 个，提供漏洞编号并提供证明（官方截图或证书加盖厂商公章）的 2 分，没有不得分。

项目 2：郑州教育管理公共服务数据安全防护项目所投“数据库防火墙”生产厂商具备《中国国家信息安全漏洞库（CNNVD）技术支撑单位》证明，并提供中国国家信息安全漏洞库官方链接与截图的，得 3 分，没有不得分。

3. 核心系统演示（25 分）

根据投标人对投标产品项目 1 “教育应用安全态势感知平台及应急支撑”进行现场演示，根据演示

效果（投标人自行准备演示环境，如需互联网请提前自行准备）进行综合比较，讲解顺序以评标现场抽签为准，演示时间为 15 分钟以内。未提供演示或采用 PPT 演示的不得分，共计 25 分，超过 4 项不满足，则演示环节不得分。

3.1 产品 1：网站立体监控平台（6 分）

①检测引擎扫描能力。可在任务设置中配置 WAF 识别功能，或在检测内容中展示 WAF 识别结果。满足得 3 分，不满足 0 分；

②域名探测功能。具备站点资产自动发现能力，任务结果可展示指定 IP 地址段内存活的 IP 地址及对应站点的属性信息。满足得 3 分，不满足 0 分。

3.2 产品 2：互联网域名安全巡管系统（6 分）

①信息展示。展示本地、近期页面篡改事件照片墙展示，可查询详情。满足得 3 分，不满足 0 分；

②爬取及检测。高亮显示爬取的网页代码，以便查看与定位篡改内容。满足得 3 分，不满足 0 分。

3.3 产品 3：互联网边界安全监测分析系统（6 分）

①资产探测与发现。展示 Web 应用进行识别结果，识别的结果须至少包含 IP 地址、标题、WEB 容器、HTTP 状态、状态持续时间、操作系统版本、CMS、开发语言、开发框架、响应时间、WEB 组件等数据。满足得 3 分，不满足 0 分；

②风险管理。展示探测出的 web 系统的敏感路径，以及敏感路径的状态监测结果，以列表或图表的方式展示。满足得 3 分，不满足 0 分。

3.4 产品 4：安全态势感知和通报预警平台（7 分）

①网络安全监控事件预警。演示通过平台下发域名巡管监控任务，展示任务结果中被黑客篡改的事件预警，可查看网站被篡改详情信息，和网站被黑快照。满足得 3 分，不满足 0 分；

②网络安全漏洞信息采集与监控。演示对开源社区监控结果，如 Github，获取关键词相关的源代码段，自动识别代码语言并实现代码高亮。满足得 2 分，不满足 0 分。

③安全预警通报及响应。演示安全预警通报 workflow，预警通报闭环处置流程至少要包含技术审核、发布管理、处理状态、归档等环节。满足得 2 分，不满足 0 分。

（四）加分项

1. 信用评估报告（1 分）：

根据郑州市财政局《郑州市政府采购中使用企业信用报告实施意见》的通知，投标人具有社会信用管理部门备案认可的信用评级机构出具的《企业信用报告》等级为 AAA 级的，得 1 分；其他不得分。

（以上需投标人提供注册地市级以上信用建设部门认可的信用评级机构出具的《企业信用报告》、查询网址，同时提供信用评级机构相应的资质材料，否则不得分）

2. 节能和环境标志（1分）

投标的主要产品载入财政部、国家发改委和国家环保部发布的最新环境标志产品政府采购清单、节能产品政府采购清单内，且在有效期内的（必须提供有关证明材料和文件，否则不得分）各加0.5分。
（政府强制采购节能产品的除外）