

河南省安全生产智能化监管平台项目

招标文件

招标编号：豫财招标采购-2020-1441

招标人：河南省应急管理厅

招标代理：河南招标采购服务有限公司

二〇二〇年十一月

目 录

第一册.....	3
第 1 章 投标人须知.....	3
一 总 则.....	3
1. 采购人、采购代理机构、投标人、政府采购监督管理部门.....	3
2. 资金来源.....	3
3. 投标费用.....	4
4. 适用法律.....	4
二 招标文件.....	4
5. 招标文件构成.....	4
6. 招标文件的澄清与修改.....	5
7. 投标截止时间的顺延.....	5
三 投标文件的编制.....	6
8. 投标范围及投标文件中标准和计量单位的使用.....	6
9. 投标文件组成.....	6
10. 证明投标标的合格性和符合招标文件规定的技术文件.....	6
11. 投标报价.....	7
12. 投标保证金.....	7
13. 投标有效期.....	7
14. 投标文件的制作.....	8
四 投标文件的递交.....	9
15. 投标文件的密封和标记.....	9
16. 投标截止.....	9
17. 投标文件的接收、修改与撤回.....	9
五 开标及评标.....	9
18. 开标.....	9
19. 资格审查及组建评标委员会.....	10
20. 投标文件符合性审查与澄清.....	11
21. 投标无效.....	13

22. 比较与评价.....	14
23. 废标.....	14
24. 保密要求.....	15
六 确定中标.....	15
25. 中标候选人的确定原则及标准.....	15
26. 确定中标候选人和中标供应商.....	15
27. 发出中标通知书.....	15
28. 告知招标结果.....	15
29. 签订合同.....	16
30. 履约保证金.....	16
31. 付款方式.....	16
32. 招标代理费.....	16
33. 政府采购信用担保.....	17
34. 廉洁自律规定.....	17
35. 人员回避.....	17
36. 质疑的提出与接收.....	17
37. 知识产权.....	18
38. 融资政策：内容详见附件 3。.....	18
附件 1：履约保证金保函（格式）.....	19
附件 2：履约担保函格式.....	20
附件 3：河南省政府采购合同融资政策告知函.....	23
第 2 章 投标文件格式.....	24
目 录.....	25
第一部分 开标一览表及资格证明文件.....	25
1 开标一览表.....	26
2 法人或者非法人组织的营业执照等证明文件或自然人的身份证明.....	27
3 法定代表人（或负责人）身份证明书.....	28
4 法定代表人（或负责人）授权委托书.....	29
5 投标保证承诺书.....	30

5.1 投标保证金承诺书.....	30
6 具有良好的商业信誉和健全的财务会计制度的承诺书.....	33
6.1 财务状况报告.....	34
6.2 依法缴纳社会保障资金和税收的证明材料.....	34
7 具备履行合同所必需的设备和专业技术能力的书面承诺（格式自拟）	35
8 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和反商业贿赂的承诺书（投标文件格式五、六）	36
9 投标须知前附表要求的其他资格证明文件.....	38
第二部分 商务及技术文件.....	39
1 投标函.....	40
2 投标报价明细表.....	42
3 商务条款偏离表.....	44
4 符合《政府采购促进中小企业发展暂行办法》、《关于政府采购支持监狱企业发展有关问题的通知》和《三部门联合发布关于促进残疾人就业政府采购政策的通知》价格扣减条件的投标人须提交资料.....	45
4-1 投标人企业（单位）类型声明函.....	46
4-2 投标人监狱企业声明函.....	47
4-3 残疾人福利性单位声明函.....	48
4-4 制造商企业（单位）类型声明函（如需要）	49
5 投标人关联单位的说明.....	50
6 2018 年 1 月 1 日以来符合本项目要求的业绩一览表.....	51
7 技术要求偏离表.....	52
8 项目实施方案.....	53
9 售后服务方案.....	54
10 投标须知前附表及评分标准中要求的其他文件.....	55
第二册.....	56
第 3 章 投标邀请.....	56
第 4 章 投标须知前附表.....	59
第 5 章 项目采购需求.....	64

一、项目背景.....	64
二、当前现状.....	65
三、采购需求.....	66
1、建设目标	66
2、建设内容	68
3、采购清单	69
四、技术要求.....	72
1、总体技术要求	72
3、总体架构要求	72
4、建设内容要求	73
五、应用系统技术指标.....	105
六、成品软件技术指标.....	107
七、安全产品技术指标.....	113
1、防火墙	114
2、主机安全加固	115
3、防病毒	116
4、数据库审计	116
5、数据库防火墙	119
6、网页防篡改	122
7、Web 应用防火墙	123
8、堡垒机	124
9、漏洞扫描	124
10、日志审计	126
11、安全管理中心	127

八、其他技术要求.....	130
九、实施要求.....	131
十、验收要求.....	132
十一、培训要求.....	132
十二、售后服务要求.....	132
十三、知识产权和保密要求.....	133
第 6 章 评标方法和标准.....	134
第 7 章 政府采购合同.....	145

特别提示

1、投标人注册及市场主体信息登记

投标人、供应商（市场主体）需要完成信息登记及 CA 数字证书办理，才能通过河南省公共资源交易中心平台参与交易活动，具体办理事宜请查阅《河南省公共资源交易中心》网站“办事指南”专区的《河南省公共资源交易平台市场主体信息库登记指南（工程建设、政府采购）》完成注册。

2、投标文件制作

2.1 投标人通过“河南省公共资源交易中心（www.hnggzy.com）”网站公共服务（办事指南及下载专区）：下载“投标文件制作工具安装包压缩文件下载”等。

2.2 投标人凭 CA 密钥登陆市场主体并按网上提示自行下载每个项目所含格式（.hznzf）的招标文件。

2.3 投标人须在投标文件递交截止时间前制作并提交：

加密的电子投标文件，应在投标文件截止时间前通过“河南省公共资源交易中心（www.hnggzy.com）”电子交易平台内上传。

2.4 加密的电子投标文件为“河南省公共资源交易中心（www.hnggzy.com）”网站提供的“投标文件制作工具”软件制作生成的加密版投标文件。

2.5 投标人编辑电子投标文件时，根据招标文件要求用法定代表人或负责人 CA 密钥和企业 CA 密钥进行签章制作；最后一步生成电子投标文件时，只能用本单位的企业 CA 密钥。

3、澄清与变更

采购人、采购代理机构对已发出的招标文件进行的澄清、更正或更改，澄清、更正或更改的内容将作为招标文件的组成部分。采购代理机构将通过网站“变更公告”和系统内部“答疑文件”告知投标人。各投标人须重新下载最新的招标文件和答疑文件，依此编制投标文件。

4、河南省公共资源交易中心平台在开标前对投标人信息具有保密性，投标人在投标文件递交截止时间前须自行查看项目进展、变更通知、澄清及回复，因

投标人未及时查看而造成的后果由投标人自行承担。

5、根据《河南省公共资源交易中心关于推行全程不见面服务的通知》要求，除必须提交样品或现场演示情况外，所有项目均采用不见面开标。投标人无需到省交易中心现场参加开标会议，投标人（供应商）应当在招标（采购）文件确定的投标截止时间前，登录远程开标大厅，在线准时参加开标活动并进行文件解密、答疑澄清、二次报价等。详见《河南省公共资源交易中心》首页-公共服务-办事指南 《河南省公共资源交易平台不见面服务系统使用指南》

按照省交易中心的要求，为了不影响投标，交易主体（投标人、供应商）务必尽快根据自己的实际情况和招标文件/采购文件（招标文件），在网上添加市场主体类型，完善各供应商主体库中的相应信息包括企业资质、业绩、人员、获奖、证书、纳税、社会保障、财务状况等采购文件（招标文件）中要求的相应资料，并对新增主体类型进行 CA 证书激活，否则可能影响投标文件/响应文件的制作，添加主体类型并激活证书后，新增主体类型的基本信息需要提交交易中心工作人员验证，验证时间为一个工作日，建议投标人（供应商）提前办理，以免影响报名及投标。市场主体登记的信息在交易中心网站“市场主体库公示”专栏对外公开，接受社会监督，登记的信息必须真实准确、合法有效，如信息填写错误或者未及时更新信息或者弄虚作假的，自行承担相应的后果及责任。

河南省公共资源交易平台不见面服务系统使用指南
<http://www.hnsggzy.com/hnsggzy/infodetail/?infoId=e70f7862-200e-4b0d-973f-bd872e9ab283&categoryNum=003003> 包括不见面服务操作手册-主体库信息（企业资质业绩人员等）补充、不见面服务操作手册-投标响应文件制作（投标人）、不见面服务操作手册-远程开标（投标人）、不见面服务操作手册-质疑异议（供应商）等，各投标人一定要仔细研究。

文件中“个人电子签章”是指个人的电子签名或个人电子章；“企业电子签章”是指企业的电子章。

第一册

第1章 投标人须知

一 总则

1. 采购人、采购代理机构、投标人、政府采购监督管理部门

1.1 采购人：是指依法进行政府采购的国家机关、事业单位、团体组织。

本项目的采购人见投标须知前附表。

1.2 采购代理机构：是指河南招标采购服务有限公司。

1.3 投标人：是指响应招标、参加投标竞争的法人、非法人组织或者自然人。

潜在投标人：以招标文件规定的方式获取本项目招标文件的法人、非法人组织或者自然人。

本项目的投标人及其投标货物须满足以下条件：

1.3.1 符合投标须知前附表中规定的投标人资格要求。

1.4 是否允许联合体投标：是

1.5 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参与本项目同一合同项下的投标的，其相关投标将被认定为**投标无效**。

1.6 为本项目提供过整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加本项目上述服务以外的其他采购活动。否则其投标将被认定为**投标无效**。

1.7 本次招标的政府采购监督管理部门：本次招标项目的采购人所属预算级次的财政部门。

2. 资金来源

2.1 本项目的采购人已获得足以支付本次招标后所签订的合同项下的资金（包括财政性资金和本项目采购中无法与财政性资金分割的非财政性资金）。

2.2 项目预算金额和最高限价（如有）见投标须知前附表。

2.3 投标人报价超过招标文件规定的预算金额或者最高限价的，其投标将被认定为**投标无效**。

3. 投标费用

不论投标的结果如何，投标人应承担所有与投标有关的费用。

4. 适用法律

本项目采购人、采购代理机构、投标人、评标委员会的相关行为均受《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》及本项目本级和上级财政部门政府采购有关规定的约束和保护。

二 招标文件

5. 招标文件构成

5.1 招标文件分为二册，共 7 章，构成如下：

第一册

第1章 投标人须知

第2章 投标文件格式

第二册

第3章 投标邀请

第4章 投标须知前附表

第5章 采购需求

第6章 评标方法和标准

第7章 政府采购合同

5.2 招标文件中有不一致的，有澄清的部分以最终的澄清更正内容为准；未澄清的，**以投标须知前附表为准**；投标须知前附表不涉及的内容，以编排在后的最后描述为准。

5.3 投标人应认真阅读招标文件所有的事项、格式、条款和技术规范等。按照招标文件要求提交全部资料。

5.4 现场考察或者答疑会及相关事项见投标须知前附表。

- 5.5 原则上采购人、采购代理机构不要求投标人提供样品。除仅凭书面方式不能准确描述采购需求，或者需要对样品进行主观判断以确认是否满足采购需求等特殊情况除外。

如需提供样品，对样品相关要求见投标须知前附表，对样品的评审方法及评审标准见招标文件第6章。

6. 招标文件的澄清与修改

- 6.1 投标人应仔细阅读和检查招标文件的全部内容。如发现缺页或附件不全，应及时向采购人提出，以便补齐。如有疑问，应在获取招标文件或招标公告期限届满之日起七（7）个工作日内在交易平台上进行提问，要求采购人对招标文件予以澄清。
- 6.2 招标文件的澄清将在投标须知前附表规定的投标截止时间前在交易平台上公布给投标人，但不指明澄清问题的来源。
- 6.3 **交易中心平台投标人信息在开标前具有保密性，投标人在投标截止时间前须自行查看项目进展、变更通知、澄清及回复，因投标人未及时查看而造成的后果自负。**
- 6.4 采购人、采购代理机构对已发出的招标文件进行的澄清或修改，澄清或修改的内容将作为招标文件的组成部分。采购代理机构将通过河南省政府采购网(<http://www.hngp.gov.cn/>)河南省公共资源交易网(www.hnggzy.com)网站“变更公告”和系统内部“答疑文件”告知投标人，各投标人须重新下载最新的答疑、澄清文件，以此编制投标文件。

7. 投标截止时间的顺延

为使投标人有足够的时间对招标文件的澄清或者修改部分进行研究而准备投标或因其他原因，采购人将依法决定是否顺延投标截止时间。

三 投标文件的编制

8. 投标范围及投标文件中标准和计量单位的使用

- 8.1 投标人可对招标文件中一个或几个包进行投标。
- 8.2 投标人应当对所投包的“采购需求”所列的所有内容进行投标，如仅响应所投包中的部分内容，其该包投标将被认定为**投标无效**。
- 8.3 无论招标文件中是否要求，投标人所投货物及伴随的服务和工程均应符合国家强制性标准。
- 8.4 除招标文件中有特殊要求外，投标文件中所使用的计量单位，应采用中华人民共和国法定计量单位。
- 8.5 **投标语言：**投标文件以及投标人所有与采购人及采购代理机构就投标来往的文件、资料均使用中文。如果投标人提供有外文资料应附有相应的中文译本，并以中文译本为准。

9. 投标文件组成

- 9.1 投标文件由“第一部分，开标一览表及资格证明文件”和“第二部分，商务及技术文件”组成。投标人应完整地按照招标文件提供的投标文件格式及要求编写投标文件。投标文件中资格审查和符合性审查涉及的事项不满足招标文件要求的，其投标将被认定为**投标无效**。
- 9.2 电子投标文件的签章：投标人必须按照招标文件的要求，签字或加盖电子章。

10. 证明投标标的合格性和符合招标文件规定的技术文件

- 10.1 投标人应提交证明文件，证明其投标标的符合招标文件规定。该证明文件是投标文件的技术文件。
- 10.2 上款所述的证明文件，可以是文字资料、图纸和数据，包括：
 - 10.2.1 货物主要技术指标和性能的详细说明及实现的功能或者目标；
 - 10.2.2 货物从买方开始使用至招标文件规定的保质期内正常、连续地使用所必须的备件和专用工具清单，包括备件和专用工具的货源及现行价格；

10.2.3 对照招标文件技术规格，逐条说明所提供货物及伴随的工程和服务已对招标文件的技术规格做出了实质性的响应，或申明与技术规格条文的偏差和例外。

10.3 本条所指证明文件不包括对招标文件相关部分的文字、图标的复制。

11. 投标报价

11.1 投标人的报价应当包括满足本次招标全部采购需求所应提供的货物，以及伴随的服务(除非在投标须知前附表中另有规定)。所有投标均应以人民币报价。

11.2 投标人应按照招标文件提供的投标报价表格式如实填写各项货物及服务的单价、分项总价和总投标报价。

11.3 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。投标人在报价中所填报的价格均包含完成该项目的全部费用，包含货物的(含相关附件、材料)价款、运输费、装卸费、配送费、检测费、保险费用、税费及其技术和售后服务费等一切有关费用，采购人无须向中标人另外支付任何费用。

11.4 如项目分包，除非招标文件另有规定，每一包只允许有一个最终报价，任何有选择的报价或替代方案将导致投标无效。

11.5 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。

11.6 投标人在报价时应考虑期间的物价上涨，政策性调整等诸多因素以及由此引起的费用变动并计入总报价。

12. 投标保证金

12.1 本项目投标人无需提交投标保证金。

13. 投标有效期

13.1 投标应在投标须知前附表中规定时间内保持有效。投标有效期不满足要

求的投标，其投标将被认定为**投标无效**。

- 13.2 因特殊原因，采购人或采购代理机构可在原投标有效期截止之前，要求投标人延长投标文件的有效期。接受该要求的投标人将不会被要求和允许修正其投标。投标人也可以拒绝延长投标有效期的要求，且不承担任何责任。上述要求和答复都应以书面形式提交。
- 13.3 投标截止时间至本项目发布中标公告为止撤销投标，应当向采购代理机构或采购人支付本项目预算金额（或最高限价）的 2%的违约赔偿金。

14. 投标文件的制作

- 14.1 投标人在制作电子投标文件时，按照河南省公共资源交易中心提供的“投标文件制作工具”制作电子投标文件。具体查询河南省公共资源交易中心网站主页办事指南及下载专区。
- 14.2 投标文件格式所要求包含的全部资料应全部制作在投标文件内，严格按照本项目招标文件中提供的所有格式如实填写（不涉及的内容除外），不应存在漏项或缺项。**投标函及投标报价一览表，须严格按照格式编辑，并作为电子开评标系统上传的依据。**
- 14.3 投标人编辑电子投标文件时，根据招标文件要求用法人 CA 密钥和企业 CA 密钥进行签章制作；最后一步生成电子投标文件时，只能用本单位的企业 CA 密钥。
- 14.4 投标人须在投标文件递交截止时间前制作并提交投标文件。
加密的电子投标文件，应在投标文件截止时间前通过“河南省公共资源交易中心（www.hnggzy.com）”电子交易平台内上传。
- 14.5 加密的电子投标文件为“河南省公共资源交易中心（www.hnggzy.com）”网站提供的“投标文件制作工具”软件制作生成的加密版投标文件。

四 投标文件的递交

15. 投标文件的密封和标记

15.1 电子投标文件的密封和标记

因采用全程不见面投标、开标、评标方式，故投标人应将电子投标文件按要求加密后上传到指定平台。

15.2 投标文件的递交

- (1) 投标人应在投标截止时间前上传加密的电子投标文件到系统的指定位置。
上传时必须得到电脑“上传成功”的确认。请投标人在上传时认真检查上传投标文件是否完整、正确。
- (2) 投标人因交易中心投标系统问题无法上传电子投标文件时，请在工作时间与河南省公共资源交易中心联系。

16. 投标截止

16.1 投标人应在投标须知前附表中规定的截止时间前，将投标文件按照“投标须知前附表”中载明的地址上传。

16.2 采购人和采购代理机构将拒绝在规定的时间内未上传、未解密的投标文件。

17. 投标文件的接收、修改与撤回

17.1 采购人和采购代理机构将按招标文件规定的时间和地点接收投标文件，具体要求投标须知前附表。

17.2 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。在投标截止时间之后，投标人不得对其投标文件做任何修改。

17.3 除投标人不足3家未开标外，采购人和采购代理机构对所接收投标文件概不退回。

五 开标及评标

18. 开标

18.1 采购人和采购代理机构将按投标须知前附表中规定的开标时间、地点和方式组织开标。

18.2 开标方式

远程开标时：

采购机构/代理机构将在“招标资料表”规定的时间和地点组织公开开标。

投标人无需到河南省交易中心现场参加开标会议，开标采用“远程不见面”开标方式，开标大厅的网址（www.hnggzyjy.cn）。投标人（供应商）须在招标（采购）文件确定的投标截止时间前，登录远程开标大厅，在线准时参加开标活动，并在规定的时间内进行文件解密、答疑澄清等。具体事宜请查阅河南省公共资源交易中心网站“办事指南”专区的《河南省公共资源交易平台不见面服务系统使用指南》。

18.3 投标人须在投标须知前附表规定的时间内完成加密投标文件解密。由于投标人的自身原因，在规定时间内解密不成功的，作**无效投标**处理。

18.5 投标人下载招标文件后，如未在招标文件规定的投标文件递交截止时间前成功上传或误传加密的投标文件，而导致的解密失败，投标将被拒绝。

18.6 开标时，系统将公布投标人名称、投标报价等开标记录表中其它内容。

18.7 投标人不足3家的，不予开标。

19. 资格审查及组建评标委员会

19.1 采购人或采购代理机构依据法律法规和招标文件中规定的内容，对投标人进行资格审查，未通过资格审查的投标人不进入评标。通过资格审查的投标人不足三家的，不得评标。

19.2 采购人或采购代理机构将按投标须知前附表中规定的时间查询投标人的信用记录。

19.2.1 投标人在中国政府采购网（www.ccgp.gov.cn）被列入政府采购严重违法失信行为记录名单，或在“信用中国”网站（www.creditchina.gov.cn）被列入失信被执行人、重大税收违法案件当事人名单，以及存在《中华人民共和国政府采购法实施条例》第十九条规定的重大违法记录，投标将被认定为**投标无效**。

19.2.2 采购人或采购代理机构经办人将查询网页打印、签字并存档备查。投标人不良信用记录以采购人或采购代理机构查询结果为准。投标人自行提

供的与网站信息不一致的其他证明材料亦不作为资格审查依据。

在本招标文件规定的查询时间之外，网站信息发生的任何变更均不作为资格审查依据。

19.3 按照《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》及本项目本级和上级财政部门的有关规定依法组建的评标委员会，负责评标工作。

19.4 评标委员会由采购人代表和评审专家组成，成员人数为七人及以上单数。其中，评审专家不得少于成员总数的三分之二。具体成员人数见投标须知前附表。

20. 投标文件符合性审查与澄清

20.1 符合性审查是指依据招标文件的规定，从商务和技术角度对投标文件的有效性和完整性进行审查，以确定是否对招标文件的实质性要求做出响应。

20.2 投标文件的澄清

20.2.1 在评标期间，评标委员会将要求投标人对其投标文件中含义不明确、对同类问题表述不一致或者有明显文字和计算错误的内容，以及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，有可能影响履约的情况作必要的澄清、说明或补正。投标人的澄清、说明或补正应在评标委员会规定的时间内进行，并不得超出投标文件范围或者改变投标文件的实质性内容。

20.2.2 投标人（供应商）应当在招标（采购）文件确定的投标截止时间前，登录远程开标大厅，在线准时参加开标活动并进行文件答疑澄清等。

20.2.3 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。

20.2.4 投标文件的澄清不得对投标内容进行实质性修改。

20.2.5 投标人的澄清、说明或补正将作为投标文件的一部分。

20.3 投标文件报价出现前后不一致的，按照下列规定修正：

(1) 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；

(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。

(5) 投标报价有算术错误的，其风险由投标人承担。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照第 20.2 条的规定经投标人确认后产生约束力，投标人不确认的，其投标将被认定为**投标无效**。

对不同文字文本投标文件的解释发生异议的，以中文文本为准。

20.4 如一个包（标段）内只有一种产品，不同投标人所投产品为同一品牌的，按如下方式处理：

20.4.1 如本项目使用最低评标价法，提供相同品牌产品的不同投标人以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会按照招标文件中评标办法规定的方式确定一个参加评标的投标人；未规定的采取随机抽取方式确定，其他投标将被认定为**投标无效**。

20.4.2 如本项目使用综合评分法，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，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供应商推荐资格；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中评标办法规定的方式确定一个投标人获得中标供应商推荐资格；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。

20.5 如一个包内包含多种产品的，采购人或采购代理机构将在**投标须知前附表**中载明核心产品，投标人提供的核心产品中只要有 1 个核心产品的品牌相同，相关投标人将被认定为属于提供相同品牌产品，按第 20.4 条规定处理。

20.6 投标人所投产品如被列入财政部与国家主管部门颁发的节能产品或环境标志产品品目清单或无线局域网产品清单，应提供处于有效期之内认证

证书等相关证明，在评标时予以优先采购，具体优先采购办法见第 6 章评标方法和标准。

如采购人所采购产品为政府强制采购的产品，投标人所投产品应属于品目清单的强制采购部分。投标人应提供有效期内的认证证书，否则其投标将被认定为**投标无效**。

如采购人所采购产品属于信息安全产品的，投标人所投产品应为经国家认证的信息安全产品，并提供由中国信息安全认证中心按国家标准认证颁发的有效认证证书，否则其投标将被认定为**投标无效**。

关于政府采购节能产品或环境标志产品的相关要求详见以下文件中的相关规定：

- ①关于印发节能产品政府采购品目清单的通知（财库〔2019〕19号）；
- ②关于印发环境标志产品政府采购品目清单的通知（财库〔2019〕18号）；
- ③国家市场监督管理总局《关于发布参与实施政府采购节能产品、标志产品认证机构名录的公告》（2019年第16号）

21. 投标无效

21.1 在比较与评价之前，根据招标文件的规定，评标委员会要审查每份投标文件是否响应了招标文件的要求。投标人不得通过修正或撤销不符合要求的偏离，从而使其投标成为实质上响应的投标。

评标委员会决定投标的响应性只根据招标文件要求和投标文件内容。

21.2 如发现下列情况之一的，其投标将被认定为**投标无效**：

- （1）投标人未按招标文件要求格式签字或加盖电子签章的；
- （2）不同投标人投标文件制作机器码一致的；
- （3）未满足招标文件中商务和技术条款的实质性要求；
- （4）属于串通投标，或者依法被视为串通投标；
- （5）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，有可能影响履约的，且投标人未按照规定证明其报价合理性的；
- （6）投标文件含有采购人不能接受的附加条件的；

(7) 属于招标文件规定的其他投标无效情形。

22. 比较与评价

- 22.1 经符合性审查合格的投标文件，评标委员会将根据招标文件确定的评标方法和标准，对其技术部分和商务部分作进一步的比较和评价。
- 22.2 评标严格按照招标文件的要求和条件进行。根据实际情况，在投标须知前附表中规定采用下列一种评标方法，详细评标标准见招标文件第 6 章：
- (1) 最低评标价法，是指投标文件满足招标文件全部要求，且投标报价最低的投标人为中标候选人的评标方法。
- (2) 综合评分法，是指投标文件满足招标文件全部要求，且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法。
- 22.3 据《政府采购促进中小企业发展暂行办法》（财库[2011]181号）、《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）和《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，对满足价格扣除条件且在投标文件中提交了《投标人企业类型声明函》、《残疾人福利性单位声明函》或省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件的投标人，其投标报价扣除 6-10%后参与评审。具体办法详见招标文件第 6 章。
- 22.4 落实其他政府采购政策条款。具体办法详见招标文件第 6 章。

23. 废标

出现下列情形之一，将导致项目废标：

- (1) 符合专业条件的供应商或者对招标文件做实质性响应的供应商不足三家；
- (2) 出现影响采购公正的违法、违规行为的；
- (3) 投标人的报价均超过了采购预算，采购人不能支付的；
- (4) 因重大变故，采购任务取消的。

24. 保密要求

- 24.1 评标将在严格保密的情况下进行。
- 24.2 有关人员应当遵守评标工作纪律，不得泄露评标文件、评标情况和评标中获悉的国家秘密、商业秘密。

六 确定中标

25. 中标候选人的确定原则及标准

除评标委员会受采购人委托直接确定中标供应商的情形外，对实质上响应招标文件的投标人按下列方法进行排序，确定中标候选人：

(1) 采用最低评标价法的，除了算术修正和落实政府采购政策需进行的价格扣除外，不对投标人的投标价格进行任何调整。评标结果按修正和扣除后的投标报价由低到高顺序排列。报价相同的处理方式详见招标文件第 6 章。

(2) 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，按修正和扣除后的投标报价由低到高顺序排列。得分与投标报价均相同的处理方式详见招标文件第 6 章。

26. 确定中标候选人和中标供应商

26.1 评标委员会将根据评标标准，按**投标须知前附表**中规定数量推荐中标候选人。

26.2 按**投标须知前附表**中规定，由评标委员会直接确定中标供应商。

27. 发出中标通知书

在投标有效期内，中标供应商确定后，采购人或者采购代理机构发布中标公告。在公告中标结果的同时，向中标供应商发出中标通知书，中标通知书是合同的组成部分。

28. 告知中标结果

在公告中标结果的同时，告知未通过资格审查投标人未通过的原因；采用综合评分法评审的，还将告知未中标供应商本人的评审得分和排序。

29. 签订合同

- 29.1 中标供应商应当自发出中标通知书之日起 30 日内，与采购人签订合同。
- 29.2 招标文件、中标供应商的投标文件及其澄清文件等，均为签订合同的依据。
- 29.3 如中标供应商拒绝与采购人签订合同的，应当向采购人支付本项目预算金额（或最高限价）2%的违约赔偿金；采购人可以按照评标报告推荐的中标候选人排序，确定下一中标候选人为中标供应商，也可以重新开展采购活动。
- 29.4 当出现法规规定的中标无效或中标结果无效情形时，采购人可与排名下一位的中标候选人另行签订合同，或依法重新开展采购活动。

30. 履约保证金

- 30.1 如果需要履约保证金，中标供应商应按照**投标须知前附表**规定向采购人提供履约保证金保函（如格式见本章附件 1）。经采购人同意，中标供应商也可以自愿采用其他履约保证金的提供方式。
- 30.2 政府采购利用担保试点范围内的项目，除 30.1 规定的情形外，中标供应商也可以按照财政部门的规定，向采购人提供合格的履约担保函（格式见本章附件 2）。
- 30.3 如果中标供应商没有按照上述履约保证金的规定执行，将被视为放弃中标资格，应当向采购人支付本项目预算金额（或最高限价）2%的违约赔偿金；在此情况下，采购人可确定下一候选人为中标供应商，也可以重新开展采购活动。

31. 付款方式

- 31.1 付款方式：验收合格后付款。

32. 招标代理费

本项目是否由中标供应商向采购代理机构支付招标代理费，按照**投标须知前附表**规定执行。

33. 政府采购信用担保

- 33.1 本项目是否属于信用担保试点范围见投标须知前附表。
- 33.2 如属于政府采购信用担保试点范围内,中小型企业投标人可以自由按照财政部门的规定,采用履约担保和融资担保。
- 33.2.1 投标人递交的履约担保函应符合本招标文件的规定。
- 33.2.2 中标供应商可以采取融资担保的形式为政府采购项目履约进行融资。
- 33.2.3 合格的政府采购专业信用担保机构见投标须知前附表。

34. 廉洁自律规定

- 34.1 采购代理机构工作人员不得以不正当手段获取政府采购代理业务,不得与采购人、供应商恶意串通。
- 34.2 采购代理机构工作人员不得接受采购人或者供应商组织的宴请、旅游、娱乐,不得收受礼品、现金、有价证券等,不得向采购人或者供应商报销应当由个人承担的费用。
- 34.3 为强化内部监督机制,供应商可按投标须知前附表中代理机构的反腐倡廉监督电话/邮箱,反映采购代理机构的廉洁自律等问题。

35. 人员回避

潜在投标人认为招标文件使自己的权益受到损害的,投标人认为采购人员及其相关人员有法律法规所列与其他供应商有利害关系的,均可以向采购人或采购代理机构书面提出回避申请,并说明理由。

36. 质疑的提出与接收

- 36.1 投标人认为招标文件、招标过程和中标结果使自己的权益受到损害的,可以根据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》和《政府采购质疑和投诉办法》的有关规定,依法向采购人或其委托的采购代理机构提出质疑。
- 36.2 质疑供应商应按照财政部制定的《政府采购质疑函范本》格式(可从财政部官方网站下载)和《政府采购质疑和投诉办法》的要求,在法定质疑期

内以书面形式提出质疑，针对同一采购程序环节的质疑次数应符合投标须知前附表的规定。

超出法定质疑期提交的质疑将被拒绝。

重复或分次提出的、内容或形式不符合《政府采购质疑和投诉办法》的，质疑供应商将依法承担不利后果。

36.3 质疑函接收部门、联系电话和通讯地址，见投标须知前附表。

37. 知识产权

37.1 投标人须保证采购人在中华人民共和国境内使用投标货物、资料、技术、服务或其任何一部分时，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律或经济纠纷。如投标人不拥有相应的知识产权，则在投标报价中必须包括合法获取该知识产权的一切相关费用。如因此导致采购人损失的，投标人须承担全部赔偿责任。

38. 融资政策：内容详见附件 3。

附件 1：履约保证金保函（格式）

（如需要中标后开具）

致：（买方名称）

_____号合同履行保函

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

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

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

谨启

出具保函银行名称：_____

签字人姓名和职务：_____

签字人签名：_____

公章：_____

附件 2：履约担保函格式

(采用政府采购信用担保形式时使用)

政府采购履约担保函(项目用)

编号:

_____ (采购单位名称):

鉴于你方与_____ (以下简称供应商)于__年__月__日签定编号为 的《_____政府采购合同》(以下简称主合同),且依据该合同的约定,供应商应在__年__月__日前向你方交纳履约保证金,且可以履约担保函的形式交纳履约保证金。应供应商的申请,我方以保证的方式向你方提供如下履约保证金担保:

一、保证责任的情形及保证金额

(一)在供应商出现下列情形之一时,我方承担保证责任:

1. 将中标项目转让给他人,或者在投标文件中未说明,且未经采购招标机构人同意,将中标项目分包给他人的;

2. 主合同约定的应当缴纳履约保证金的情形:

(1) 未按主合同约定的质量、数量和期限供应货物/提供服务/完成工程的;

(2) _____。

(二)我方的保证范围是主合同约定的合同价款总额的_____%数额为

元(大写_____),币种为_____。(即主合同履约保证金金额)

二、保证的方式及保证期间

我方保证的方式为:连带责任保证。

我方保证的期间为:自本合同生效之日起至供应商按照主合同约定的供货/完工期限届满后____日内。

如果供应商未按主合同约定向贵方供应货物/提供服务/完成工程的,由我方在保证金额内向你方支付上述款项。

三、承担保证责任的程序

1. 你方要求我方承担保证责任的，应在本保函保证期间内向我方发出书面索赔通知。索赔通知应写明要求索赔的金额，支付款项应到达的帐号。并附有证明供应商违约事实的证明材料。

如果你方与供应商因货物质量问题产生争议，你方还需同时提供_____部门出具的质量检测报告，或经诉讼（仲裁）程序裁决后的判决书、调解书，本保证人即按照检测结果或判决书、调解书决定是否承担保证责任。

2. 我方收到你方的书面索赔通知及相应证明材料，在_____个工作日内进行核定后按照本保函的承诺承担保证责任。

四、保证责任的终止

1. 保证期间届满你方未向我方书面主张保证责任的，自保证期间届满次日起，我方保证责任自动终止。保证期间届满前，主合同约定的货物\工程\服务全部验收合格的，自验收合格日起，我方保证责任自动终止。

2. 我方按照本保函向你方履行了保证责任后，自我方向你方支付款项（支付款项从我方账户划出）之日起，保证责任即终止。

3. 按照法律法规的规定或出现应终止我方保证责任的其它情形的，我方在本保函项下的保证责任亦终止。

4. 你方与供应商修改主合同，加重我方保证责任的，我方对加重部分不承担保证责任，但该等修改事先经我方书面同意的除外；你方与供应商修改主合同履行期限，我方保证期间仍依修改前的履行期限计算，但该等修改事先经我方书面同意的除外。

五、免责条款

1. 因你方违反主合同约定致使供应商不能履行义务的，我方不承担保证责任。

2. 依照法律法规的规定或你方与供应商的另行约定，全部或者部分免除供应商应缴纳的保证金义务的，我方亦免除相应的保证责任。

3. 因不可抗力造成供应商不能履行供货义务的，我方不承担保证责任。

六、争议的解决

因本保函发生的纠纷，由你我双方协商解决，协商不成的，通过诉讼程序解决，诉讼管辖地法院为_____法院。

七、保函的生效

本保函自我方加盖公章之日起生效。

保证人：（公章）

年 月 日

附件 3：河南省政府采购合同融资政策告知函

各供应商：

欢迎贵公司参与河南省政府采购活动！

政府采购合同融资是河南省财政厅支持中小微企业发展，针对参与政府采购活动的供应商融资难、融资贵问题推出的一项融资政策。贵公司若成为本次政府采购项目的中标成交供应商，可持政府采购合同向金融机构申请贷款，无需抵押、担保，融资机构将根据《河南省政府采购合同融资工作实施方案》（豫财购〔2017〕10 号），按照双方自愿的原则提供便捷、优惠的贷款服务。

贷款渠道和提供贷款的金融机构，可在河南省政府采购网“河南省政府采购合同融资平台”查询联系。

第2章 投标文件格式

投标文件封面

格式可由投标人自拟

河南省安全生产智能化监管平台项目

投 标 文 件

招标编号：豫财招标采购-2020-

投标人（企业电子签章）：

法定代表人或负责人（个人电子签章）：

日 期： 年 月 日

目 录

第一部分 开标一览表及资格证明文件

目 录

1. 开标一览表（投标文件格式一）
2. 法人或者非法人组织的营业执照等证明文件扫描件（须盖章）或自然人的身份证明扫描件
3. 法定代表人（或负责人）身份证明书（投标文件格式二）
4. 法定代表人（或负责人）授权委托书（投标文件格式三）
5. 投标保证承诺书（投标文件格式四）
6. 具有良好的商业信誉和健全的财务会计制度的承诺书
7. 具备履行合同所必需的设备和专业技术能力的证明材料
8. 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和反商业贿赂承诺书的承诺书（投标文件格式五、六）
9. 投标须知前附表要求的其他资格证明文件

1 开标一览表

金额单位：元

投标人名称	
投标总报价	大写： _____
	小写： _____
工期	
质量保证期	
投标保证金	无
投标有效期	
其他声明	

投标人（企业电子签章）：

2 法人或者非法人组织的营业执照等证明文件或自然人的身份证明

投标人应提供资料：

说明：1. 提供有效的营业执照等证明文件扫描件。

2. 投标人为自然人的，应提供身份证明扫描件。

3. 联合体投标应提供联合体各方满足以上要求的证明文件。

3 法定代表人（或负责人）身份证明书

（投标文件格式二）

投标人名称：_____ 单位性质：_____

地址：_____

成立时间：____年____月____日 经营期限：_____

姓名：_____性别：____年龄：____职务：_____系_____（投标人名称）的法定代表人（或负责人）。

特此证明。

投标人：_____（企业电子签章）

详细通讯地址：_____ 邮 政 编 码：_____

电 话：_____ 电 子 邮 箱：_____

日 期：____年____月____日

注：自然人投标的无需提供

（下面应附法定代表人或负责人身份证扫描件正反面）

投标人（企业电子签章）：_____

详细通讯地址：_____

邮 政 编 码：_____

电 话：_____

注：自然人投标的无需提供

法定代表人（或负责人）身份证（A面）	法定代表人（或负责人）身份证（B面）
--------------------	--------------------

4 法定代表人（或负责人）授权委托书

(投标文件格式三)

本人_____（姓名）系_____（投标人名称）的法定代表人（或负责人），现委托 _____（姓名）为我单位的合法代理人。代理人根据授权，就（项目名称）投标，以我单位名义处理一切与之有关的事务，其法律后果由我单位承担。

委托期限： 20 **年**月**日至 20**年**月**日(填写具体日期)。

投标人： _____（企业电子签章）

法定代表人或负责人（签字或个人电子签章）： _____

详细通讯地址： _____

邮 政 编 码： _____

电 话： _____

电 子 邮 箱： _____

日 期： _____年_____月_____日

注：自然人投标的或法定代表人或负责人投标的无需提供

（下面应附代理人身份证扫描件正反面）

被委托人身份证（A面）	被委托人身份证（B面）
-------------	-------------

5 投标保证金承诺书

(投标文件格式四)

5.1 投标保证金承诺书

致（采购人及采购代理机构）：

我公司作为本次采购项目的投标人，根据招标文件要求，现郑重承诺如下：

一、具备《中华人民共和国政府采购法》第二十二条第一款和本项目规定的条件：

- （一）具有独立承担民事责任的能力；
- （二）具有良好的商业信誉和健全的财务会计制度；
- （三）具有履行合同所必需的设备和专业技术能力；
- （四）有依法缴纳税收和社会保障资金的良好记录；
- （五）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；
- （六）法律、行政法规规定的其他条件；
- （七）根据采购项目提出的特殊条件。

二、完全接受和满足本项目招标文件中规定的实质性要求，如对招标文件有异议，已经在投标截止时间届满前依法进行维权救济，不存在对招标文件有异议的同时又参加投标以求侥幸中标或者为实现其他非法目的的行为。

三、参加本次招标采购活动，不存在与单位负责人为同一人或者存在直接控股、管理关系的其他供应商参与同一合同项下的政府采购活动的行为。

四、参加本次招标采购活动，不存在为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的行为。

五、参加本次招标采购活动，不存在和其他供应商在同一合同项下的采购项目中，同时委托同一个自然人、同一家庭的人员、同一单位的人员作为代理人的行为。

六、投标人参加本次政府采购活动要求在近三年内投标人和其法定代表人没有行贿犯罪行为。

七、投标文件中提供的能够给予我公司带来优惠、好处的任何材料资料和技术、服务、商务等响应承诺情况都是真实的、有效的、合法的。

八、如本项目评标过程中需要提供样品，则我公司提供的样品即为中标后将要提

供的中标产品，我对提供样品的性能和质量负责，因样品存在缺陷或者不符合招标文件要求导致未能中标的，我愿意承担相应不利后果。（如提供样品）

九、存在以下行为之一的愿意接受相关部门的处理：

- （一）投标有效期内撤销投标文件的；
- （二）在采购人确定中标人以前放弃中标候选资格的；
- （三）由于中标人的原因未能按照招标文件的规定与采购人签订合同；
- （四）由于中标人的原因未能按照招标文件的规定交纳履约保证金；
- （五）在投标文件中提供虚假材料谋取中标；
- （六）与采购人、其他供应商或者采购代理机构恶意串通的；
- （七）投标有效期内，投标人在政府采购活动中有违法、违规、违纪行为。

如果发生任何一项以上行为，将在该行为发生的 10 个工作日内，向贵方（或采购人）支付本招标文件公布的预算金额或最高限价（如无预算金额或最高限价的话，以我单位的投标报价为基准）的 2%作为违约赔偿金。

承认本承诺书作为贵方（或采购人）要求我单位履行违约赔偿义务的依据作用。

由此产生的一切法律后果和责任由我公司承担。我公司声明放弃对此提出任何异议和追索的权利。

本公司对上述承诺的内容事项真实性负责。如经查实上述承诺的内容事项存在虚假，我愿意接受以提供虚假材料谋取中标追究法律责任。

投标人（企业电子签章）： _____

日期： _____

5.2 招标代理服务费承诺函

致（采购人及采购代理机构）：

我们在贵公司组织的（项目名称：_____，采购代理编号：_____）招标中若获中标，我们保证在中标公告发布后 5 个工作日内，按招标文件的规定，以支票、银行转账、汇票或现金，向贵公司一次性支付招标代理服务费用。否则，由此产生的一切法律后果和责任由我公司承担。

承认本承诺书作为贵方要求我单位履行违约赔偿义务的依据作用。

我公司声明放弃对此提出任何异议和追索的权利。

特此承诺。

投标人（企业电子签章）：_____

日期：_____

6 具有良好的商业信誉和健全的财务会计制度的承诺书

说明：

1. 投标人承诺本单位具有良好的商业信誉和健全的财务会计制度（格式自拟）。
2. 如果是联合体投标，联合体各方均需提供承诺书。

投标人（企业盖章或电子签章）：

年 月 日

6.1 财务状况报告

说明：1. 会计师事务所或审计部门出具的 2018 或 2019 年度财务审计报告或银行出具的资信证明或财政部门认可的政府采购专业担保机构出具的投标担保函。

如提供财务审计报告应提供完整的财务审计报告。

注：参考《财政部关于注册会计师在审计报告上签名盖章有关问题的通知》（财会【2001】1035 号）规定，审计报告应当由两名具备相关业务资格的注册会计师签名盖章并经会计师事务所盖章方为有效。

2. 如果是联合体投标，联合体各方均需提供上述资料。

6.2 依法缴纳社会保障资金和税收的证明材料

说明：

1. 2019 年 6 月以来任意 3 个月的依法纳税证明和缴纳社保证明。

2. 如果是联合体投标，联合体各方均需提供上述资料。

7 具备履行合同所必需的设备和专业技术能力的书面承诺（格式自拟）

（若为联合体投标，联合体各方均需提供上述资料）

**8 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和反商业贿赂的
承诺书（投标文件格式五、六）**

8.1 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承诺书

我公司承诺：

我公司近三年内在中华人民共和国境内经营活动中没有重大违法记录，具有良好的商业信誉和完善的售后服务体系，并能承担招标项目供货能力和服务的企业。

若我公司承诺不属实，同意取消本项目参加资格，并将承担相关法律责任，接受处理。

说明：1. 投标人应按照相关法规规定如实作出承诺。

2. 如果是联合体投标，联合体各方均需提供上述证明。

投标人（企业盖章或电子签章）：

年 月 日

8.2 反商业贿赂承诺书

我单位承诺：

在 （投标项目名称） 招标活动中，我公司保证做到：

- 一、公平竞争参加本次招标活动。
- 二、杜绝任何形式的商业贿赂行为。不向国家工作人员、政府采购代理机构工作人员、评审专家及其亲属提供礼品礼金、有价证券、购物券、回扣、佣金、咨询费、劳务费、赞助费、宣传费、宴请；不为其报销各种消费凭证，不支付其旅游、娱乐等费用。
- 三、若出现上述行为，我公司及参与投标的工作人员愿意接受按照国家法律法规等有关规定给予的处罚。

说明：1. 投标人应按照相关法规规定如实作出承诺。

2. 如果是联合体投标，联合体各方均需提供上述证明。

投标人（企业盖章或电子签章）：

年 月 日

9 投标须知前附表要求的其他资格证明文件

说明：1. 应提供投标须知前附表要求的其他资格证明文件。

2. 如果是联合体投标，联合体各方需提供的满足招标文件要求的其他资格证明文件。

第二部分 商务及技术文件

1. 投标函
2. 商务条款偏离表
3. 符合《政府采购促进中小企业发展暂行办法》、《关于政府采购支持监狱企业发展有关问题的通知》和《三部门联合发布关于促进残疾人就业政府采购政策的通知》价格扣减条件的投标人须提交资料
 - 3-1 《投标人为中小企业（单位）声明函》
 - 3-2 《投标人监狱企业声明函》
 - 3-3 《残疾人福利性单位声明函》
 - 3-4 《制造商投标人企业（单位）类型声明函》
4. 投标人关联单位的说明（格式自拟）
5. 2018年1月1日以来符合本项目要求的业绩一览表
6. 项目实施方案
7. 售后服务方案
8. 投标须知前附表及评分标准中要求的其他文件

1 投标函

(投标文件格式七)

致：_____（采购代理机构名称）

我们获取了采购编号为_____的_____（项目名称）采购文件，经详细研究，我们决定参加该项目的投标活动并按要求提交投标文件。我们郑重声明以下诸点并负法律责任：

根据贵方（项目名称）项目的投标邀请（招标编号），签字代表（姓名、职务）经正式授权并代表投标人（名称、地址）提交投标文件。

据此，签字代表宣布同意如下：

- （1）愿按照采购文件中规定的条款和要求，提供完成采购文件规定的全部工作。
- （2）本投标有效期为自投标截止之日起60个日历日。
- （3）已详细审查全部招标文件，包括所有补充通知（如果有的话），完全理解并同意放弃对这方面有不明、误解的权利。
- （4）我方不是为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，我方不是采购代理机构的附属机构。
- （5）按照招标文件的规定，在中标后向贵方一次性支付招标代理费。
- （6）按照贵方可能的要求，提供与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。
- （7）按照招标文件的规定履行合同责任和义务。
- （8）完全理解并无条件承担中标后不依法与采购人签订合同的法律后果。

与本投标有关的一切正式往来信函请寄：

地址：_____ 传真：_____

固定电话：_____ 授权代表移动电话：_____

电子邮箱：_____

投标人（企业电子签章）：_____

投标人开户银行（全称）： _____

投标人银行帐号： _____

日期： _____

2 投标报价明细表

2.1 软件定制开发服务部分报价

报价单位：元

序号	定制开发内容	单价	数量	小计
1				
2				
3				
.....				
合计：				

注：该表中工作内容可自行调整，内容可自行细化。

2.2 硬件及成品软件部分报价

报价单位：元

序号	所投产品名称	品牌/型号	产地	单价	数量	小计
1						
2						
3						
.....						
合计：						

注：该表中工作内容可自行扩展，内容可自行细化。

2.3 其他报价

序号	类别	单价	数量	小计	备注
1	集成				
2	运维				
3	培训				
.....					
合计：					

注：该表中工作内容可自行扩展，内容可自行细化。

投标人：_____（企业电子签章）
日期：_____年_____月_____日

3 商务条款偏离表

项目名称：

招标编号：

序号	招标文件条款号	招标文件的商务条款	投标文件的商务条款	说明
1	工期			
2	付款方式			
3	质保期			
4	投标有效期			
5	….			
	其他			

投标人（企业电子签章）：

4 符合《政府采购促进中小企业发展暂行办法》、《关于政府采购支持监狱企业发展有关问题的通知》和《三部门联合发布关于促进残疾人就业政府采购政策的通知》价格扣减条件的投标人须提交资料

4-1 投标人企业（单位）类型声明函

本企业（单位）郑重声明下列事项（按照实际情况勾选或填空）：

1、本企业（单位）为直接投标人，提供本企业（单位）制造的货物。

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

（2）本企业（单位）为联合体一方，提供本企业（单位）制造的货物，由本企业（单位）承担工程、提供服务。本企业（单位）提供协议合同金额占到共同投标协议合同总金额的比例为_____。

2、本企业（单位）为代理商，提供其他_____（请填写：大型、中型、小型、微型）企业、监狱企业或残疾人福利性单位制造的货物。本条所称货物不包括使用大型企业注册商标的货物。（后附制造商企业（单位）类型声明函）

本企业（单位）对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标人（企业电子签章）：

日期：_____

4-2 投标人监狱企业声明函

本企业（单位）郑重声明下列事项（按照实际情况勾选或填空）：

本企业（单位）为直接投标人提供本企业（单位）制造的货物。

（1）本企业（单位）_____（请填写：是、不是）监狱企业。后附省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

（2）本企业（单位）_____（请填写：是、不是）为联合体一方，提供本企业（单位）制造的货物，由本企业（单位）承担工程、提供服务。本企业（单位）提供协议合同金额占到共同投标协议合同总金额的比例为_____。

本企业（单位）对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标人（企业电子签章）：

日 期：_____

4-3 残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加_____单位的_____项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标人（企业电子签章）：

日 期： _____

4-4 制造商企业（单位）类型声明函（如需要）

本企业（单位）作为_____单位的_____项目（投标人名称）所投设备的制造商，参加政府采购活动。根据《政府采购促进中小企业发展暂行办法》（财库[2011]181号），《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）、《财政部、司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）以及《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的有关规定，作出如下声明：

本企业为_____（请填写：大型、中型、小型、微型）企业。

本企业_____（请填写：是、不是）监狱企业。后附省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

本单位_____（请填写：是、不是）残疾人福利性单位。

本企业（单位）提供本企业（单位）制造的货物。

本企业（单位）对上述声明的真实性负责。如有虚假，将依法承担相应责任。

本声明函经制造商和投标人共同盖公章生效。

制造商（盖章）：_____

投标人（盖章）：_____

日期：_____

注：投标人所投产品均为自己制造，可不提供此声明函。

5 投标人关联单位的说明

(格式自拟)

说明：投标人应当如实披露与本单位存在下列关联关系的单位名称：

- (1) 与投标人单位负责人为同一人的其他单位；
- (2) 与投标人存在直接控股、管理关系的其他单位。
- (3) 若为联合体投标，联合体各方均应提供本说明。

6 2018年1月1日以来符合本项目要求的业绩一览表

序号	项目名称	项目类型	合同金额	签订时间	项目单位联系人电话

注：投标人需附相关项目的完整合同并加盖电子签章。

（此表可延长）

投标人(企业电子签章)：

日 期：

7 技术指标偏离表

项目名称：

招标编号：

序号	分项名称	招标要求	投标响应	偏差描述	结论

投标人：_____（企业电子签章）

日期：_____年_____月_____日

注：投标内容和招标要求有偏离的应在“偏离表”中列明。若无偏离，可在偏离表中描述“无偏离”。

8 项目实施方案

(格式自拟)

投标人（企业电子签章）：

日期：

9 售后服务方案

(培训及售后服务) (格式自拟)

投标人 (企业电子签章) :

日期:

10 投标须知前附表及评分标准中要求的其他文件

第二册

第3章 投标邀请

河南省安全生产智能化监管平台项目招标公告

项目概况

河南省安全生产智能化监管平台项目的潜在投标人应在河南省公共资源交易中心平台获取招标文件，并于 2020 年 12 月 21 日 9 点 00 分（北京时间）前递交投标文件。

一、项目基本情况

- 1、项目编号：豫财招标采购-2020-1441
- 2、项目名称：河南省安全生产智能化监管平台
- 3、采购方式：公开招标
- 4、预算金额：4045.4 万元人民币，最高限价：3761 万元人民币
- 5、采购需求：

河南省安全生产智能化监管平台建设项目依托河南省省级政务云、省电子政务外网建设，平台主要覆盖省、市、县三级应急管理机构，实现省、市、县三级应用，由省级统一部署，各市县根据当地实际进行相关功能的补充和完善建设。计算、存储和网络资源由省级政务云支撑满足。主要采购内容为：

- (1) 数据资源管理系统；
- (2) 应用支撑系统；
- (3) 五大业务域应用系统；
- (4) 安全系统；
- (5) 标准规范；

(6) 完成与河南省“互联网+监管”系统、河南省政务服务网及其他相关系统的对接服务等。

还包括上述建设内容涉及的需求调研、软硬件采购、开发实施、交付验收、系统培训、运行维护等相关服务工作。

本项目建设周期为 20 个月。项目验收通过之日起，成品软硬件产品质保期 3 年，定制开发的软件维护服务期 2 年。

6、合同履行期限：自合同签订之日起 20 个月

7、本项目是否接受联合体投标：（是）

8、是否接受进口产品：（否）

二、申请人的资格要求：

1. 满足《中华人民共和国政府采购法》第二十二条的规定；

2. 落实政府采购政策需满足的资格要求：无。

3. 本项目的特定资格要求：无。

三、获取招标文件

1、供应商须完善河南省公共资源交易中心市场主体信息库登记并取得 CA 密钥，凭 CA 密钥登陆市场主体系统并按网上提示下载招标文件及资料（详见 <http://www.hnggzy.com> 公共服务-办事指南）。

2、招标文件下载时间为 2020 年 11 月 30 日至 2020 年 12 月 4 日（北京时间），供应商未按规定在网上下载招标文件的，其投标将被拒绝。

3、获取招标文件后，供应商请到河南省公共资源交易中心网站—公共服务—下载专区栏目下载最新版本的投标文件制作工具安装包，并使用安装后的最新版本投标文件制作工具制作电子投标文件。

4. 售价：免费下载，不收取费用

四、投标截止时间及地点

1. 时间：2020 年 12 月 21 日 9 时 00 分（北京时间）

2. 地点：河南省公共资源交易中心远程开标室(一)-8

3. 投标人按规定在河南省公共资源交易中心网站上传加密电子投标文件，加密电子投标文件逾期上传将不予受理。

五、开标时间及地点

1. 时间：2020 年 12 月 21 日 9 时 00 分（北京时间）
2. 地点：河南省公共资源交易中心远程开标室(一)-8
3. 其他有关事项：投标人进行远程解密（投标人须提前进入远程开标大厅（<http://www.hnggzy.com/>）进行开标操作和投标文件的解密。具体操作流程及程序，请投标人查阅河南省公共资源交易平台“办事指南”专区的《河南省公共资源交易平台不见面服务系统使用指南》。）

六、发布公告的媒介及招标公告期限

本次招标公告在《河南省政府采购网》、《河南省公共资源交易中心网》上发布。

招标公告期限为五个工作日。

七、其他补充事宜：（无）

八、凡对本次招标提出询问，请按照以下方式联系。

1. 采购人信息

名称：河南省应急管理厅

地址：郑州市纬二路 10 号

联系人：姚老师

联系方式：0371-65919752

2. 采购代理机构信息

名称：河南招标采购服务有限公司

地址：郑州市纬四路 13 号 315 室

联系人：李芬、张斯栋

联系方式：0371-65958908

3. 项目联系方式

项目联系人：李芬

联系方式：0371-65958908

发 布 人：河南招标采购服务有限公司

发布时间： 2020 年 11 月 27 日

第4章 投标须知前附表

本表是本招标项目的具体资料，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。

条款号	内 容
1.1	采购人：河南省应急管理厅 地 址：河南省郑州市纬二路 10 号 联系人：姚老师 联系电话：0371-65919752
1.2	采购代理机构：河南招标采购服务有限公司 地址：郑州市金水区纬四路 13 号 业务联系人：李芬、张斯栋 联系方式：0371-65958908 电子邮箱：2207495218@qq.com
1.3.1	*投标人资格要求： 1. 满足《中华人民共和国政府采购法》第二十二条的规定； 2. 落实政府采购政策需满足的资格要求：无。 3. 本项目的特定资格要求：无。
1.3.5	是否允许采购进口产品：否
1.3.6	是否为专门面向中小企业采购：否
1.4	是否允许联合体投标：是
2.2	项目预算金额：4045.4 万元。最高限价：3761 万元。投标报价超出最高限价，按无效投标处理。
5.4	是否组织现场考察或者召开答疑会：否 组织现场考察或者召开答疑会相关要求：无
5.5	是否需要提供样品：否
6.1	获取招标文件或招标公告期限届满之日起七（7）个工作日内，在河南

	省公共资源交易平台上进行提问，同时将问题的电子版以电子邮件形式发送至邮箱：2207495218@qq.com, (附加盖企业公章的扫描件和 Word 电子版)。
6.3	投标人在河南省公共资源交易中心平台自行查看，因投标人未及时查看而造成的后果自行承担。
9.1	<p>资格证明文件（电子投标文件中必须附以下资料原件的扫描件或复印件的扫描件）：</p> <ul style="list-style-type: none"> *1. 有效期的营业执照； *2. 法定代表人身份证明书、法定代表人授权委托书（附本人身份证扫描件及授权投标代表身份证）； *3. 投标保证承诺书； *4. 投标人财务状况报告（2018 或 2019 年度的财务审计报告，财务审计报告应具有 2 名及以上注册会计师盖章和签字。成立时间不足 1 年的，提供银行出具的资信证明或财政部门认可的政府采购专业担保机构出具的投标担保函）； *5. 投标人 2019 年 6 月 1 日以来任意 3 个月纳税证明材料和社会保障资金缴纳相关材料； *6. 具有履行合同所必需的设备和专业技术能力的书面承诺； *7. 投标人提供参加政府采购活动前三年内在经营活动中没有重大违法、违纪行为书面声明； *8. 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的声明函。 <p>【如有投标人成立时限不足要求时限的，由投标人根据自身成立时间提供相关证明资料；在法规范围内不需提供的，应出具书面说明和证明文件】。</p>
11.1	(1) 投标报价：报价应是采购人指定地点交货价，包含完成该项目的全部费用。包含软件开发所有费用、成品软件及硬件设备（含相关附件、材料）价款、运输费、装卸费、配送费、检测费、保险费用、税

	<p>费及其技术和售后服务费等等一切有关费用，采购人无须向中标人另外支付任何费用。投标报价应结合采购预算、运保费、服务、中标服务费等。</p> <p>最终合同支付金额为目的地交货价（包含本项目所采购服务及设备费用、运保费、各种服务等）。</p> <p>(2)相关费用：由中标人承担的费用，包括招标服务费等相关费用。</p>
13.1	*投标有效期：提交投标文件截止之日起 <u> 60 </u> 日历日
16.1	投标截止时间：2020年12月21日9时00分（北京时间）
18.1	<p>开标时间：同投标截止时间</p> <p>开标地点：河南省公共资源交易中心远程开标室(一)-8</p>
18.2	加密的电子投标文件解密时间：投标截止时间后的30分钟内。
19.2	<p>信用信息截止时间点：同投标截止时间；</p> <p>信用查询时间：投标截止时间开始查询。</p> <p>*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）《河南省财政厅关于转发财政部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的通知》（豫财购〔2016〕15号）的规定，在“信用中国”网站查询供应商“失信被执行人”和“重大税收违法案件当事人名单”，在“中国政府采购”网站查询供应商“政府采购严重违法失信行为记录名单”；如果投标供应商存在不良信用记录的，其投标文件将被作为无效处理。</p> <p>查询及记录方式：采购人或采购代理机构经办人将查询网页打印、签字并存档备查。投标人不良信用记录以采购人或采购代理机构查询结果为准。投标人自行提供的与网站信息不一致的其他证明材料亦不作为资格审查依据。</p>
19.4	<p>评标委员会成员人数：7人，由经济、技术专家和采购人代表等组成。</p> <p>除采购人代表以外的外聘专家不少于评委会成员所有成员的三分之二，并按政府采购制度的规定从财政部门的政府采购专家库中随机抽</p>

	取。
20.5	核心产品：本项目主要采购内容为软件开发服务，不适用核心产品认定。
20.6	1、采购产品被列入财政部与国家主管部门颁发的节能产品或环境标志产品品目清单或无线局域网产品清单：否 2、采购产品为政府强制采购的产品：否 *3、根据《关于调整信息安全产品强制性认证实施要求的公告》（2009年第33号）、《关于信息安全产品实施政府采购的通知》（财库〔2010〕48号）要求，本次涉及产品：防火墙、数据库审计、数据库防火墙、Web应用防火墙、堡垒机、漏洞扫描、日志审计，必须为经国家认证的信息安全产品，提供由中国信息安全认证中心按国家标准认证颁发的有效认证证书。
22.2	评标方法：适用 <u>综合评分法</u>
26.1	推荐中标候选人的数量： <u>3名</u>
26.2	采购人是否委托评标委员会直接确定中标供应商： <u>否</u>
30.1	是否提交履约保证金： <u>是</u> 履约保证金金额：合同金额的2%。 履约担保的形式：现金、转账或保函。 履约保证金的交纳方式：中标人在领取中标通知书后、签订合同前向采购人提供。 履约保证金的退还：系统软件完成开发并验收合格，资料正式交接完毕，交付采购人使用后，予以退还。
31.1	付款方式：签订合同后采购人支付合同额20%；初验完成后采购人支付合同额50%；终验完成后采购人支付合同额25%；质保金为合同额的5%，按照成品软硬件3年质保、定制开发软件系统2年质保的期限，质保期内每年质保验收合格后支付该年度对应的质保金。
32	是否由中标供应商缴纳招标代理费： <u>是</u> 。

	<p>招标代理费：按照中标金额的 1%向中标人收取。由中标人在领取中标通知书前向招标代理机构缴纳。</p> <p>中标供应商在领取中标通知书前将招标代理费交至河南招标采购服务有限公司，账户信息如下：</p> <p>开户行：广发银行郑州行政区支行</p> <p>户名：河南招标采购服务有限公司</p> <p>帐号：8898516010005452</p> <p>财务室联系电话：0371-65955702</p>
33.1	本项目是否属于信用担保试点范围： <u>否</u>
34.3	<p>采购代理机构反腐倡廉监督电话：<u>0371—6596 2573</u></p> <p>邮 箱：<u>hnzbcggs2000@126.com</u></p>
36.2	<p>针对同一采购程序环节的质疑次数：<input checked="" type="checkbox"/> 一次性提出</p> <p><input type="checkbox"/> 多次提出</p>
36.3	<p>质疑函接收</p> <p>联系部门：<u>河南招标采购服务有限公司 六部</u></p> <p>联系人员：<u>李芬、张斯栋</u></p> <p>联系电话：<u>0371-65958908</u></p> <p>通讯地址：<u>河南省郑州市金水区纬四路 13 号 315 室</u></p>

第5章 项目采购需求

一、项目背景

党的十八大以来，习近平总书记对应急管理工作多次作出重要论述，强调要牢固树立灾害风险管理和综合减灾理念，坚持以防为主、防抗救相结合，坚持常态救灾和非常态救灾相统一，努力实现“三个转变”，全面提升全社会抵御自然灾害的综合防范能力。特别是2018年10月10日，总书记主持召开中央财经委员会第三次会议进行研究，并发表重要讲话，指出“加强自然灾害防治关系国计民生，要建立高效科学的自然灾害防治体系，提高全社会自然灾害防治能力，为保护人民群众生命财产安全和国家安全提供有力保障”，这些为做好相关工作指明了前进方向，提供了根本遵循。

中国共产党第十九届中央委员会第四次全体会议从推进国家治理体系和治理能力现代化的高度，明确了应急管理工作必须坚持和巩固的根本点、完善和发展的方向，并作出工作部署，并明确指出“完善和落实安全生产责任和管理制度，建立公共安全隐患排查和安全预防控制体系。构建统一指挥、专常兼备、反应灵敏、上下联动的应急管理体制，优化国家应急管理能力体系建设，提高防灾减灾救灾能力”。

在中共中央政治局第十九次集体学习中习总书记强调：“要发挥我国应急管理体系的特色和优势，借鉴国外应急管理有益做法，积极推进我国应急管理体系和能力现代化，提出要强化应急管理装备技术支撑，优化整合各类科技资源，推进应急管理科技自主创新，依靠科技提高应急管理的科学化、专业化、智能化、精细化水平。要适应科技信息化发展大势，以信息化推进应急管理现代化，提高监测预警能力、监管执法能力、辅助指挥决策能力、救援实战能力和社会动员能力”。

《应急管理部关于加快编制地方应急管理信息化发展规划的通知》中指出，省级应急管理部门要重点加强源头信息采集和业务系统建设，主要包括四个方面：一是大力开展监测预警感知网络建设，实现安全生产、自然灾害、应急资源等信息的采集，提高实时监测、动态分析、预测预警能力。二是不断扩大信息获取范围，分类接入气象、自然资源、水利、文通运输、森林等外部单位信息资源。三是建设应急管理综合应用平台，对各类数据资源进行自动汇聚、关联、融合，并按要求实时汇入应急管理

大数据应用平台。四是建设应急指挥调度等业务系统，与应急管理大数据应用平台的相关模块实现高效协同。

为推动并指导地方应急发展，应急管理部 2019 年下发 11 项地方任务书，2020 年下发 8 项地方建设任务书。

建立健全社会预警体系，有效应对各种风险，预防和减少自然灾害、事故灾难、公共卫生和社会安全事件及其造成的损失，保障人民群众生命财产安全、维护社会稳定，既是人民政府根本宗旨的必然要求，也是全面提高政府管理和服务社会能力的重要任务。现阶段，我国经济迅速发展、社会大局稳定，当前国际国内应急管理形势不容乐观，各种影响国家和社会稳定的因素依然存在。各级应急管理部门一定要站在落实科学发展观、提高党的执政能力和构建和谐社会的高度，充分认识加强应急管理工作的重要性和紧迫性，切实增加责任感和紧迫感。

二、当前现状

近两年，云计算、物联网、人工智能、大数据、“互联网+”等新概念、新技术、新模式、新应用不断涌现，在实现政务信息资源集约化发展、促进信息共享方面形成巨大推力，带来了许多新方法、新思路。云计算为信息化建设提供了集约化发展的平台，云计算降低了建设成本、建设周期，增强了部署的敏捷性、灵活性和系统可集成性。物联网则是政府监管和企业监控之间的桥梁，物联网的出现和广泛应用，填补了政府监管向企业延伸的技术鸿沟，通过物联网技术，实现应急管理数据自动采集，政府部门着力于物联网数据采集标准制定、巡查监管和大数据应用，从而实现态势监测和预警，实现监管执法与事故救援数据追溯和评估。

河南省委、省政府高度重视应急管理信息化建设工作，对信息化建设做出明确安排和部署，就提高河南省安全生产信息化建设水平、构建“智慧应急”管理体系等工作专门召开会议，进行了具体的业务指导和部署。加快推进应急管理领域的信息化建设，是完成党中央国务院、河南省委省政府交办任务，要求应急管理厅不折不扣加紧落实。

为响应河南省委、省政府和应急管理部对应急管理信息化建设的要求，省应急管理厅迅速组织力量进行“智慧应急”平台的升级与规划，基于河南省安全生产智能化监管平台快速实现各业务系统的统一认证、集约化管理，实现应急管理信息化系统一体化管理；充分利用云计算、物联网、大数据等当前主流的互联网技术，实现数据融合，从数据融合着手，创新应用，促进业务融合与扩展提升，快速实现“智慧应急”平台的一体化、智慧化的扩展升级。

应急管理各转隶部门多针对安全生产、洪涝、地震、森林火灾、草原火灾等单一灾害、涉及要素较少等问题。如今，应急管理部面临着多灾种、多要素、全过程综合性应急救援难题，承担着跨领域、跨层级综合指挥调度的重任，纵向、专一的系统完全无法满足复杂形势的迫切需求，亟需将新一代信息技术与应急管理职能相结合，补短板，强弱项，填空白，破难题，全面提升应急救援的协同性、整体性、专业性，提高国家防灾减灾救灾能力，防范化解重大安全风险，形成统一领导、权责一致、权威高效的国家应急能力体系，推进应急管理现代化。

目前河南省应急管理厅自建 18 个业务应用系统，主要是基于原安监局业务开展，为多个厂家分别建设，系统应用效果不一，系统基本属于独立运行，缺乏统一的支撑平台及数据处理机制，且应急管理厅改革成立之后，目前业务系统无法满足新的职责业务要求，需要在此基础上进行新建、改造及整合。另外使用部级统建系统 2 个，为危化品监测预警系统、尾矿库监测预警系统。

三、采购需求

1、建设目标

深入贯彻落实习近平总书记关于应急管理、防灾减灾救灾、安全生产系列重要论述，全面提升河南省自然灾害防治、安全生产预防和应急管理能力，充分利用物联网、大数据、地理信息及人工智能技术，构建全省统一标准、整合共享的应急管理数据资源管理系统，融合创新的技术支撑平台体系，围绕监督管理、监测预警、指挥救援、

决策支持、政务管理业务域打造智慧协同的应急管理业务应用体系，纵向贯通省、市、县三级应急管理机构，横向整合各转隶单位相关系统，快速形成应急管理一体化综合应用平台；基于数据汇聚融合与业务协同，深入开展大数据分析智能创新应用，充分运用应急管理“大数据”分析预警能力和“物联网”动态感知能力，提高应急管理效能，打造应急管理“一张图”、感知监测“一张网”、布设应急资源“一盘棋”、实现救援指挥“一平台”，服务企业、社会公众、应急管理机构三个群体，形成“智慧应急”的新格局，并为下一步的业务深度融合与业务创新打下基础。

(1) 建设一套标准规范体系，标准规范的建设使得信息具有统一性和唯一性，以此达到对河南省安全生产智能化监管平台的标准化管理，统一标准规范有利于实现应用系统的整合和优化，从而最大程度实现河南省各级应急管理机构信息数据资源的集成与共享，指导全省应急管理信息化建设，保证各项应急管理业务流程的畅通。

(2) 建设统一的全省智慧应急业务应用体系，建立监督管理、监测预警、指挥救援、决策支持、政务管理 5 大业务域，支撑常态、非常态下的事前、事发、事中、事后全过程业务开展，为各级各类用户提供集成化应用服务。

(3) 建设先进强大的数据支撑体系，构建全方位获取、全网络汇聚、全维度整合的海量数据资源治理体系，汇聚、接入各涉灾涉险部门的数据资源，满足精细治理、分类组织、精准服务、安全可控的数据资源管理要求。为全灾种风险防范，大应急决策指挥提供数据支撑。

(4) 建设稳定、安全的应用支撑体系，建设应用支撑平台，为应用系统提供基于微服务框架的基础支撑组件、开发框架、服务总线等基础支撑，为统一标准、快速构建提供平台支持。

(5) 建设安全保障体系，通过防火墙、主机安全加固、防病毒、数据库审计、数据库防火墙、网页防篡改、Web 应用防火墙、堡垒机、漏洞扫描、日志审计等安全设备的采购部署，充分保障安全生产智能化监管平台的数据安全、应用安全。

2、建设内容

河南省安全生产智能化监管平台主要建设一套标准规范，一个数据资源管理系统提供数据资源支撑，一个应用支撑为整个平台提供了应用开发环境、应用集成环境、系统运行保障等公共应用服务，监督管理、监测预警、指挥救援、决策支持、政务管理五大业务域，满足安全生产及应急管理业务需求，建设安全系统，按照国家要求保障系统数据安全。

(1) 应用系统

监督管理业务域：围绕应急管理厅监督管理职责需要，基于深化“放管服”改革及提高监督执法检查效率的需要，对行政许可系统、行政执法系统进行升级改造，新建安全生产培训考试系统、双重预防体系系统。

监测预警业务域：主要实现对自然灾害、安全生产、多灾种耦合等风险的全面监测预警，提升监测信息的可信度，保障预警信息的快速及时发布，为灾害及安全事故监督管理、以及应急响应提供信息支撑，本期项目主要是围绕安全生产风险评估、自然灾害预警数据汇集两个方面进行建设。

指挥救援业务域：围绕贯穿全流程的值班值守等业务，事发、事中、事后各阶段的业务，构建指挥救援全流程业务功能。系统功能主要包括应急指挥信息系统、结构化预案管理系统、应急资源管理系统。

决策支持业务域：依托数据资源管理系统及应用支撑平台，汇聚各类监测预警数据、监督管理数据、指挥救援数据、政务管理数据等，进行风险监测预警的全面态势感知，结合大数据分析挖掘和人工智能进行辅助分析，进行灾害事故综合研判，并通过闭环反馈逐步进行决策优化，为领导提供辅助决策支撑，系统主要包括智能云搜、态势感知、辅助分析、综合研判、决策优化系统。

政务管理业务域：面向应急管理各级各类用户及社会群众，构建应急管理服务内网门户及应急管理社会服务系统。

(2) 数据资源管理系统

数据资源管理系统主要是利用数据库直接抽取、接口对接等主要采集方式，实现应急管理厅内部数据整合，本期项目主要整合对接气象、地震、农业（蓝天卫士）、旅游（景点监控）、公安（雪亮工程）、林业、民政、市场监管、交通（危化运输）、消防 10 个单位相关的数据，实现数据汇聚之后的标准化处理及相关应用支撑。其主要建设内容包括信息资源规划、数据治理、数据应用及数据接入等。

（3）应用支撑平台

应用支撑平台是应急管理厅整合汇集所有业务系统、应用支撑和数据支撑所形成的综合性集成平台，面向所有用户提供“一站式”访问入口。主要建设内容包括基础支撑软件（微服务网关、统一用户、统一授权、统一组织机构管理、统一门户等）、移动服务平台及服务开放系统等。

（4）安全系统

基于河南省政务云的实际情况，为保障应用系统安全，需采购相关安全设备，保障河南省安全生产智能化监管平台的应用安全、数据安全等。

（5）标准规范编制

依据国标、行业标准及应急管理部制定并下发的相关信息化标准，结合河南省安全监管平台建设实际需求，梳理应用系统建设、信息资源标准、数据共享标准、系统接口规范等标准规范内容，通过标准化的操作指南，实现应急管理的标准化、流程化实施。

3、采购清单

序号	分项名称	采购需求	数量	单位
一	软件开发			
1	应用系统	包括监督管理、监测预警、指挥救援、决策支持、政务服务五大业务域。	1	套
二	成品软件采购			

序号	分项名称	采购需求	数量	单位
1	支撑软件产品	支持对从简单到复杂的数据结构中的大量数据进行收集、集成和转换基础工具	1	套
2	数据资源管理系统	数据资源管理系统建设,主要是围绕应急管理的业务需要,构建数据接入、数据处理、数据资源池、数据服务、数据应用等体系,提供数据资源支撑。	1	套
3	应用支撑系统	应用支撑平台建设主要包括基础支撑软件、移动服务平台、服务开放系统、系统对接整合等建设内容。	1	套
三	安全产品采购			
1	防火墙	1U 机型,单电源,三层吞吐量 5G,并发连接数:260 万,集成访问控制、应用层威胁防护等一系列网络安全功能,满足虚拟化云环境在云边界的安全域隔离、访问控制、威胁防护、失陷检测和安全管理等需求系统;三年硬件保修和技术支持服务。	2	台
2	主机安全加固	提供 50 个虚拟化主机安全轻代理防护能力,集主机防火墙、主机入侵防御、Hypervieor 层防护、主机加固、webshell 检测于一体,支持 Windows2008 R2 X64、Windows2012 R2 X64 或 Linux 上部署。	2	套
3	防病毒	提供 50 个虚拟主机杀毒能力,有效查杀主机上的文件、内存、进程中的恶意程序,对主机进行统一的病毒查杀管理,制定定时查杀任务,辅以主动防护引擎和文件监控	2	套
4	数据库审计	2U,提供数据库操作行为审计、事件追踪、威胁分析、实时告警等多种功能,三年硬件保修和技术支持服务。	1	台
5	数据库防火墙	2U,多因子认证、屏蔽直接访问数据库的通道、攻击检测和保护、连接监控、虚拟补丁、报表、安全审计,三年硬件保修和技术支持服务。	1	台

序号	分项名称	采购需求	数量	单位
6	网页防篡改	对 Web 站点目录提供全方位的保护，防止黑客、病毒等对目录中的网页、电子文档、图片等任何类型的文件进行非法篡改和破坏	1	套
7	Web 应用防火墙	1U 机型，单电源，三层吞吐量 3G，http 并发连结数 20W，保证 Web 应用合法流量的正常传输，保障业务系统的运行连续性和完整性。实时拦截各种 WEB 攻击，能有效拦截各种 SQL 注入，XSS 跨站类型的 WEB 攻击。	1	台
8	堡垒机	1U 设备，单电源，包含 50 台设备资产安全配置检查和变更检查授权，三年硬件保修和技术支持服务。	2	台
9	漏洞扫描	1U 设备，单电源，最大并发扫描 50 个，提供资产管理、系统漏扫、网站漏扫、数据库漏扫、基线配置核查、弱口令扫描等功能。三年硬件保修和技术支持服务。	2	台
10	日志审计	1U 设备，单电源，含 50 个主机审计许可证书，处理性能 3000 条/秒，三年硬件保修和技术支持服务。	2	台
11	安全管理中心	<p>响应中心：提供安全摘要报表、主机威胁报表、脆弱性分析报表、报表个性化订阅、安全设备联动配置与管理等能力。</p> <p>智能安全分析：可检测如 webshell 后门、黑链、勒索行为、慢速扫描等，相比规则类检测，机器学习可以提高检测的准确率。</p> <p>通报预警：包括安全告警、处置工单、统计分析、工单处理流程管理、工单编辑等。</p> <p>智能安全分析：可检测如 webshell 后门、黑链、勒索行为、慢速扫描等，相比规则类检测，机器学习可以提高检测的准确率。</p> <p>通报预警：包括安全告警、处置工单、统计分析、工单处理流程管理、工单编辑等。</p> <p>日志审计/检索：可检索、查看、审计安全日志、操作记录、FLOW 形式的数据源等。</p> <p>综合管理：对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。</p>	1	套

序号	分项名称	采购需求	数量	单位
四	标准规范			
1	标准规范	系统开发规范、文件编制规范、软件管理规范、分类与编码规范、信息模型、数据项和值域范围、数据质量规范、数据交换格式、数据发布规范、共享系统运行规范、系统接口标准编写规范、感知数据交换规范、视频监控联网技术要求	1	套

四、技术要求

1、总体技术要求

以规范和创新管理作为“智慧应急”项目总体设计的出发点和落脚点；要深化需求分析，做好需求调查，以“需求为导向、应用促发展”作为项目总体设计指导性方针；技术路线的选择要突出实用性、安全性、先进性原则，重点采用成熟技术，做到节约、实用、好用，不片面追求技术的先进性；要强化资源整合，注重统筹开发，围绕互联互通和信息共享，集成、整合各级、各类业务应用系统和数据库系统，统筹好已有系统与在建系统、各类与各级系统之间的关系。

总体设计方案应当具备明显的实用性、经济性、先进性、易用性、可扩充性、开放性特征，遵循统一的标准规范，支持信息与服务高度共享。

3、总体架构要求

依托河南省政务云，在统一的安全保障体系、运维保障体系和标准规范体系保障下，采用云端集中部署，省市县企及成员单位依权限全网应用模式，构建纵向从省到市、县、级应急管理机构，横向打通气象、水利、消防、公安、交通等应急管理相关单位，前端到高危行业（领域）企业，涵盖应急管理、行业领域、中介机构、企业、社会公众的一体化、集约化的、开放包容的架构，同时充分考虑到对原有业务系统、各转隶单位信息化系统的一体化集成管理，实现统一门户展现；做好数据汇聚、对接、

共享；以数据资源管理系统为基础，做好各转隶单位原有业务系统数据的整合、相关单位的数据共享；做好各转隶部门已建系统及数据云迁移工作，保证迁移工作的平滑过渡；并充分利用大数据分析工具，从大数据分析层面，做好辅助决策支撑，促进业务创新。

4、建设内容要求

4.1 软件开发

4.1.1 监督管理业务域

监督管理业务域基于原安全监管局的信息化建设成果，针对应急管理部新的业务需求，进行补充建设和升级改造，满足河南省应急管理部门生产经营监管、安全生产监督管理、生产执法和安全生产考试需求。

4.1.1.1 行政许可四级十同

本次的目的是实现“四级十同”下的“一网通办”，同时，完成与省政府投资在线审批平台、省政务服务网的集成与数据回流。

4.1.1.1.1 许可流程功能改造

将河南省应急管理综合业务系统（以下简称“综合业务系统”）接入省政务服务平台，省、市、县三级应急管理部门统一使用综合业务系统，开展网上受理、审批，实行“前台综合受理、后台分类审批、统一窗口出件”。功能包括企业申请、线上受理、材料审核、不通过整改、许可审批、颁证送达、材料归档。

4.1.1.1.2 事项清单调整

将原事项对应关系停用，从新按照河南省应急管理厅‘四级十同’的行政许可事项清单梳理事项对应关系。确保系统中的事项与调整后的事项一一对应。

4.1.1.1.3 事项要素调整

事项要素调整包括事项名称调整、事项办理阶段调整、事项办理时限调整、事项办理申请材料清单、申请材料格式调整。

4.1.1.1.4 省政务服务平台对接

省政务服务平台对接包括单点登录对接、许可事项对接、许可事项企业申请数据回流、许可事项受理初审补正数据回流、许可事项企业补正数据回流、许可事项受理初审通过数据回流、许可事项受理初审不通过数据回流、许可事项审查人审查阶段挂起数据回流、许可事项审查人审查阶段恢复数据回流、许可事项监管部门负责人审核通过数据回流、许可事项监管部门负责人审核不通过数据回流、许可事项分管领导签批通过数据回流、许可事项分管领导签批不通过数据回流、应急预案备案数据回流、重大危险源备案数据回流。

4.1.1.1.5 省在线审批平台对接

省在线审批平台对接包括企业申报、数据接收、业务受理、内部审批、业务办结、审批事项预受理、受理初审补正数据回流、企业补正数据回流、受理初审通过数据回流、审查人审查挂起数据回流、审查人审查恢复数据回流、监管部门负责人审核通过数据回流、监管部门负责人审核不通过数据回流、分管领导签批通过数据回流、分管领导签批不通过数据回流、批复回传数据回流。

4.1.1.2 行政执法系统

政执法管理系统以移动互联等新技术应用为突破口，将网站、执法终端等渠道进行整合一体化，对行政执法过程中产生的信息以计算机和互联网电子信息的方式记载、传输、保存、再现以及批改和确定，实现行政执法信息电子化，为安监执法人员提供一个统一规范的信息化行政执法管理平台，以提高行政执法效率和质量。解决移动执法终端在信号无法覆盖的情况下，实现执法人员利用移动端对执法情况进行录入，并增加执法统计报表。

4.1.1.2.1 离线移动执法应用

离线移动执法应用主要用于满足执法人员在执法过程中遇到无网络信号覆盖的情况下依旧可实现移动执法业务应用。离线移动执法应用包含以下几点功能：离线登录、离线首页、企业登记、企业信息列表、企业信息离线编辑、检查记录编辑、隐患登记、检查情况编辑、离线检查记录列表、离线数据上传。

4.1.1.2.2 执法统计报表

根据要求，执法统计报表包括人员情况统计表、单位企业表、安全监管监察机构基本情况统计表、生产经营单位基本情况按行业统计表、生产经营单位基本情况统计表、安全生产现场执法检查统计表、安全生产监督执法评价表。

4.1.1.3 安全生产培训考试系统

安全生产培训考试系统业务覆盖安全生产培训和安全生产考试业务需求。

安全生产培训主要完成监管机构通过线上、线下等多种方式对企业相关人员对于安全生产相关的法律法规、政策、常识进行培训，帮助企业人员提高安全保障意识，加强生产安全。

4.1.1.3.1 安全生产培训子系统

安全生产培训子系统充分发挥各级政府部门、生产经营单位、培训机构的作用，利用互联网，优化配置各类资源，实现全员安全培训。功能包括用户和权限管理、配置管理、在线学习、在线测验、测验成绩管理、资源管理、培训证书管理、课件开发工具、课件传输工具、课件录制工具、问卷调查。

4.1.1.3.2 安全生产考试子系统

系统围绕网上在线考试、考生注册、考点管理、监考管理、考评管理、证书发放及诚信管理等，包括从报名考试到领取证书等流程，实现全过程的管理，提高考试效率，增强客观公正性。功能包括：考生管理、考试中心管理、考点管理、在线考试、监考管理、考评管理、证书管理、报表管理、诚信管理、系统管理、移动应用、系统

接口、数据迁移。

4.1.1.4 双重预防体系系统

结合《河南省深化安全生产风险隐患双重预防体系建设行动方案》，结合省内现有业务系统，紧密贴合双重预防机制建设业务要求，进行系统建设。主要是汇集企业安全生产台账数据，摸清安全风险与隐患底数，掌握风险与隐患实时状态，定期开展安全生产风险监管巡查，动态掌握生产安全形势。

4.1.1.4.1 监管巡查

实现对企业安全生产风险分级管控和隐患排查治理体系以及政府监管执法闭环监测跟踪，进行综合研判预警。功能包括风险点档案、风险管控监管、风险扫描、隐患监督检查、在线巡查、网格化监管。

4.1.1.4.2 双重预防辅助分析

双重预防辅助分析包括统计分析、风险时空一张图。通过对高发隐患风险点、风险排查情况、风险管控质量等多维度进行分析，并将不同行业、地区、种类、等级的风险与隐患以时间与空间两个维度进行分析，并在地图上进行展现。

4.1.1.4.3 工作考核

针对企业上报信息的质量和隐患排查工作情况进行量化考核，针对监管部门监管情况进行工作量化考核。分析工作完成度，敦促企业和监管部门完成相应的工作任务，保证风险隐患排查治理工作质量。功能包括：数据质量考核、企业内部考核、企业工作考核、监管效能考核。

4.1.1.4.4 企业双重预防体系

建设企业风险分级管控与隐患排查治理双重预防体系系统，为企业提供风险辨识与隐患排查工具，灵活定制满足企业实际需要的流程与辨识评估方法，实现企业风险隐患闭环管理。

4.1.1.4.5 双重预防体系 APP

双重预防体系 APP 在监管巡查、双重预防辅助分析功能基础上，建设移动 APP 满足企业风险隐患填报和政府监管巡查的移动需求。

4.1.2 监测预警业务域

4.1.2.1 三维可视化监管

从应急管理部门重点关注的危险化学品企业中选取 4 个试点企业进行框架式的人工建模，其中包括厂房内主要基础设施设施的适应性建模，重点监管对象和场景的真实模拟，探索三维地图应用，在“战时”能够更加准确和真实的反映事故现场情况，对实现高效、真实的应急救援指挥具有重要意义。

4.1.2.1.1 倾斜摄影 3cm 建模

通过高效的数据采集设备及专业的数据处理流程生成的数据成果更加直观反映地物的外观、位置、高度等属性，为真实效果和测绘级精度提供保证。

4.1.2.1.2 数据精修

在模型自动生成完成后，部分区域需要通过第三方软件编辑来进行修正。编辑完成后重新导回到模型生成软件拼接或融合处理。

4.1.2.1.3 单体矢量标注

倾斜摄影建模完成后将生成完整的三维场景，为了便于完成查看重点建筑的基本属性参数，需要对重点建筑物进行矢量面的标注。

4.1.2.1.4 数据优化入库

为保证数据加载的速度及相关效果，将最终生成的模型经由 Builder 软件进行优化处理，将原始数据按照金字塔结构进行统一处理与保存。

4.1.2.1.5 基于脚本的三维动态事件推演

通过脚本驱动，实现各类灾害事件的发展过程、应急救援保障措施等的三维可视

化仿真推演，实现三维场景的自动切换。

4.1.2.1.6 有害物质扩散三维模拟与分析

实现有害物质扩散三维模拟与分析功能，在高分辨率卫星影像叠加重点污染企业精细三维模型，实现污染源的精准定位与三维显示。

4.1.2.1.7 真三维立体展示功能

立体显示大屏与真三维立体展示软件功能，二者配合实现真三维立体场景的观看。

4.1.2.2 安全生产风险评估系统

以现有危化品、尾矿库风险系统数据、双重预防信息系统、指挥救援业务数据为支撑，构建风险监测指标体系和风险评估模型，利用大数据、人工智能等技术手段，建设安全生产风险评估系统，主要包括安全生产数据综合汇聚子系统、安全生产风险智能评估子系统、安全生产预警信息分析子系统和安全生产风险一张图子系统。

4.1.2.2.1 安全生产数据综合汇聚子系统

充分利用现有风险监测预警系统，通过接入现有危险化学品安全生产风险监测预警系统、尾矿库安全生产风险监测预警系统数据，融合安全生产风险要素数据及相关共享数据，实现安全生产相关基础数据、监测数据、指挥救援数据、网络舆情等数据的汇聚融合。

4.1.2.2.2 安全生产风险智能评估子系统

安全生产风险智能评估是针对不同场景通过评估指标体系、评估分析模型，利用信息化手段实现对风险隐患监测数据等各类数据的有效整合和关联分析，对事故风险（危化品罐区火灾、泄露、爆炸）、区域应急能力和区域风险等进行有针对性的综合分析和评估。

4.1.2.2.3 安全生产预警信息分析子系统

通过对接入危化企业、尾矿库企业安全生产监测预警系统的预警信息、预警响应时间、预警处置动作进行分析，挖掘企业预警信息变化规律，研判预警响应时间是否

及时，分析预警处置是否合乎要求。包括预警信息规律分析、预警响应时效分析、预警处置分析。

4.1.2.2.4 安全生产风险一张图子系统

实现各类风险信息、动态风险、风险评估结果的可视化展现。支持分类调阅、叠加分析，便于应急管理者更及时准确掌握风险发生、发展趋势、影响结果及处置过程，为突发事件分析研判工作提供辅助。

4.1.2.3 自然灾害监测预警系统

自然灾害监测预警系统接入其他行业部门部分灾害预警数据、历史灾害数据、自然灾害背景信息、基础背景空间数据等，实现气象、地震、水利等部分预警数据汇集，并实现对特定范围目标的预警信息精准推送，形成预警信息数据一张图可视化，为自然灾害监测预警信息化工程提供部分数据支撑。

4.1.2.3.1 自然灾害数据汇聚子系统

自然灾害数据汇聚子系统在接入相关专业部门预警数据基础上，通过数据治理实现数据接入、数据处理，通过数据服务提供数据共享交换服务，实现信息汇聚、共享，展示气象、水利、地震等部门的预警数据，为自然灾害预警信息综合展示提供信息服务。自然灾害数据汇聚子系统包括自然灾害预警信息接入、底图数据接入、预警信息数据治理功能。

4.1.2.3.2 自然灾害预警信息综合展现子系统

基于气象、水利、地震等自然灾害预警信息，实现河南省内自然灾害相关信息的综合展示，包括相关业务厅局所提供的数据产品综合展示，承灾体、救援物资、人员等信息的叠加。全面提升综合监测预警能力，支撑实现对各类自然灾害的早发现、早预警和早处置，提升河南省自然灾害防控能力。包括自然灾害预警综合展现一张图、风险形势统计功能。

4.1.2.3.3 灾害风险预警信息推送子系统

汇集行业部门预警预报信息，可运用应急管理部门自有发布渠道或其他渠道，对特定范围目标用户，实现预警信息及时精准推送。功能包括人员维护、预警信息推送渠道选择、预警信息推送、预警信息归档。

4.1.3 指挥救援业务域

4.1.3.1 应急指挥信息系统

应急指挥信息系统包括值班值守系统、突发事件报送系统、综合汇聚分析展示系统、协同会商系统、辅助决策（综合研判）系统、指挥调度系统、信息推送（发布）系统、业务应用移动化、培训演练系统、应急（总结）评估系统、应急指挥体系管理系统、指挥中心门户。

4.1.3.1.1 值班值守系统

落实值班排班和应急值守信息报告制度，实现值班信息的准确报送和及时处理，满足应急指挥中心值班值守业务需求。主要包括值班人员管理、值班日报/要情编辑、值排班、值班统计等功能。

4.1.3.1.2 突发事件报送系统

解决目前应急管理部门报送突发事件方式的局限性，充分发挥信息化工具的优势，在原应急管理综合业务系统上增加了适用于全省范围内的突发事件报送系统，包括待签收管理、事件报送管理、突发事件统计、业务配置等功能。

4.1.3.1.3 综合汇聚分析展示系统

针对应急指挥相关业务数据，对汇聚信息进行综合展示，主要展现信息概览、并支持从业务种类、数据总量、数据更新频率等维度展现数据情况，并在数据汇聚过程中提供监控功能，可动态查看数据及其他综合信息的汇聚情况。

综合汇聚分析展示系统具体功能如下：信息综合汇聚、多图层集成智能检索、应急指挥一张图。

4.1.3.1.4 协同会商系统

实现各级应急指挥中心、相关单位指挥中心、现场指挥中心及现场案例搜索、历史查看、图片展示、地图标注、多方协同、音视频会商、文件共享、上下联动等功能。

4.1.3.1.5 辅助决策（综合研判）系统

辅助决策的目的是根据相关预案，利用预测分析和研判结果，结合应急组织体系、工作流程、现场应急救援力量、应急救援物资等情况，通过综合应急指挥系统对有关政策法规、安全技术要求以及处理类似事件的案例等进行智能检索和分析，并结合专家意见，提供应对突发事件的指导流程和辅助决策方案。

主要包括智能方案、方案流转、方案要素管理、方案管理、知识辅助分析。

4.1.3.1.6 指挥调度系统

应急指挥调度系统旨在提升河南省应急管理厅应急业务管理和应急智能决策能力，为河南省应急管理提供强大的技术支撑。省级建设部署应用，下级地市根据自身需求进行建设，地市应急指挥信息系统与省级指挥调度系统相互共享相关信息，接收应急管理厅下达的任务信息并进行反馈。功能包括：资源需求分析、指挥调度管理、应急指挥方案、应急救援管理、设备管理、应急资金管理、应急任务管理、应急预案调看、扁平化指挥、分析研判、总结回溯（任务跟踪反馈）、灾后重建管理。

4.1.3.1.7 信息推送（发布）系统

汇集本部门安全生产及行业部门的自然灾害预警灾情信息，根据不同类型预警和灾情等级，运用应急管理部门自有发布渠道或其他渠道，对特定范围目标用户，实现预警灾情信息及时精准推送。同时，根据未来应急管理部门职责需要，预留预警灾情信息发布相关功能接口。

主要包括预警灾情信息汇总、信息推送、推送渠道管理、推送策略管理、推送信息统计等功能。

4.1.3.1.8 移动应急平台系统

移动应急平台系统支持将系统对接移动端多媒体通信云服务实现“云+端”联动，基于移动端应用提供要情报告、文件收发、值班安排、数据管理查看、全省应急态势展示、移动视频会议接入、地理信息系统。

4.1.3.1.8 培训演练系统

培训演练主要提供演练计划管理、演练场景设置、演练再现管理、演练评估管理、教育培训管理、操作演练、应急通信演练、演练总结等基础管理功能，通过突发事件的实战演练，基于平台各业务子系统实现信息接报、分析研判、事件处置、总结评估等，从而实现整个事件处置的演练。

4.1.3.1.9 应急（总结）评估系统

应急评估针对整个应急处置过程，提供应急处置相关内容的主要过程记录，作为领导和专家对事件处置评估的客观依据；处置结束后，针对事件处置过程进行总结，按照时间节点、按照处置步骤，生成总结报告。主要功能包括过程再现管理、评估模型管理、应急评估管理、总结报告管理等功能。

4.1.3.1.10 应急指挥体系管理系统

根据河南省应急管理体系和应急响应职责，结合事故灾害类型和应急预案，通过对指挥体系内各级各类型机构、人员、通讯方式等信息的管理，包括指挥体系构建、信息自动关联、信息快速检索、群组管理、信息交互功能。

4.1.3.1.11 指挥中心门户

作为应急指挥中心业务系统总入口，建立地市应急指挥中心二级门户，实现应急指挥的关键信息展示。

4.1.3.2 结构化预案管理系统

结构化预案管理实现应急预案编制流程的信息化处理，有助于提高预案编制和预案备案的管理水平。

4.1.3.2.1 结构化应急预案

提供预案编制、预案发布、应急演练、企业应急预案备案申请、企业应急预案备案审核、预案查询统计等功能。

4.1.3.2.2 应急预案备案配置

包括审核审批人库、流程时间配置等功能。

4.1.3.3 应急资源管理系统

应急资源管理系统包括应急资源普查系统、应急保障管理系统。

4.1.3.3.1 应急资源普查系统

开发全省应急资源大普查线上填报系统。系统分为政府端和非政府端两个入口，政府端用户涵盖全省各级人民政府、各级应急管理部门及安委会成员单位等，非政府端用户涵盖全省具有应急资源的企、事业单位，社会组织、团体等。政府端分为非政府单位管理、应急资源管理、系统管理功能。非政府端分为单位基本信息管理和应急救援管理。

4.1.3.3.2 应急保障管理系统

应急保障对全省应急基础数据的统一管理；提供基础数据的多维查询及基于图表的统计分析，并实现基础数据查询，以及基于地图的直观展示，方便应急人员掌握应急基础数据基于空间的分布和统计情况。包括应急保障物资、应急保障设备、应急避难场所、应急保障专家、救援队伍与装备、应急保障交通运输、医疗卫生保障、通讯保障、资金保障管理、治安维护保障、储备库管理、保障统计分析等管理功能。

4.1.3.4 专题研判系统

充分利用大数据挖掘分析技术，通过多灾种耦合及次生、衍生灾害演化模拟模型，实现事故灾害发展趋势分析、事故影响后果分析、次生衍生灾害分析、灾情损失评估等功能，快速关联、汇聚事故灾害相关信息，对事故灾害进行分析研判，指导科学施救。主要包括次生衍生灾害分析、事故灾害趋势分析、灾情损失评估等功能。

4.1.3.4.1 事故灾害发展趋势分析

基于灾害综合监测的感知数据、各部门单灾种预测预报结果，结合历史灾害基础数据，从时间维度和空间维度进行多风险耦合、次生风险预测分析。

4.1.3.4.2 事故影响范围分析

根据不同事故种类及特点，识别存在的危险危害因素，分析事故可能产生的直接后果以及次生、衍生后果，评估各种后果的危害程度和影响范围，以便做出防范措施。

4.1.3.4.3 人员疏散方案

利用人口疏散模型，确定人员紧急疏散方案，及时疏导事故区域的人员。

4.1.3.4.4 灾情损失评估

结合现场灾情数据、灾情报送数据，对受灾人口、房屋倒损、农作物受灾情况等快速评估，实现灾情指标快速评估。

4.1.3.4.5 次生衍生灾害分析

结合事故影响范围、持续时间、后果严重程度等信息，按规范生成次生、衍生事故及影响范围分析报告，并制作成次生衍生事件风险服务信息。

4.1.3.4.6 应急需求估算

计算应急处置所需资源，为资源调度提供参考。

4.1.4 决策支持业务域

4.1.4.1 智能云搜系统

以数据资源管理系统汇聚的海量数据为基础，通过关键词提取、NLP 自然语言分析与映射等，实现对相关业务信息快捷、即时、多维度的查询展现，利用二维码加密技术与识别技术，根据安全生产企业统一信用代码，对企业进行赋码，作为信息查询、信息上报、统计分析的便捷入口，并根据业务属性建立全息企业档案及应用、一人一档、一点一档。

4.1.4.1.1 智能搜索引擎

提供整合式的搜索框，支持接近自然语言的搜索条件，对大数据库中所整合的全部资源进行快速检索。

4.1.4.1.2 数据智能标签

通过抽象和提炼企业的特征标识，定义标签并构建企业标签模型。

4.1.4.1.3 一企一档一码

通过在线填报、接入汇聚企业信息，建立企业档案，支持根据安全生产企业统一信用代码，对企业进行安全码赋码，安全码作为企业身份唯一标识，可通过手机扫描，查看企业安全相关企业档案。通过数据挖掘、清洗、分析、聚合、建模，形成企业的安全生产全景画像，提供真实且快速的一站式信息查询功能。提供主体赋码、监管企业画像、关联图谱、安全监管关键指标（KPI）、企业档案、企业档案信息完整度核查校验等功能。

4.1.4.1.4 一人一档

对企业关键岗位人员信息进行汇集整理。

4.1.4.1.5 一点一档

将风险点的基本信息进行汇总展示。

4.1.4.2 态势感知系统

感知全省气象、水利、地震等自然自然灾害及危化、尾矿库行业安全生产等方面的风险态势、监测态势、预警态势、灾害态势、事故态势、舆情态势等态势；感知危化、金属非金属矿、工贸企业分布态势；感知安全生产事故变化态势；感知企业安全状态预警态势。为领导提供全面综合的态势感知视图。

4.1.4.2.1 综合态势感知

综合态势感知包括风险态势感知、监测态势感知、预警态势感知、灾害态势感知、事故态势感知、舆情态势感知、态势感知地图操作服务。

4.1.4.2.2 行业变化态势分析

包括危化品重大危险源态势预警、危化品企业地域变化态势分析、金属非金属矿地域分布态势分析、工贸企业地域分布态势分析。

4.1.4.2.3 事故变化态势分析

包括事故等级标注展现、事故类型占比对比、事故变换趋势统计、引起事故因素可视化统计功能。

4.1.4.2.4 企业安全状态预警

企业安全生产预警应具体包括以下几个功能操作流程：预警指标选择、预警指标量化、预警指标权重确定、预警模型建立、预警指数图生成、预警报告发布。

4.1.4.3 辅助分析系统

基于常态下的监督管理和历史事故灾害指挥救援的总结评估，基于常态与非常态下应急管理的决策进行优化调整，以达到对监测预警、监督管理、指挥救援、政务管理整体决策优化和流程提升。

4.1.4.3.1 专家决策分析

实现对专家各类信息的统一管理维护，为辅助决策方案提供支撑。

4.1.4.3.2 案例情景再现

汇总国内外突发事件案例分析。

4.1.4.3.3 知识辅助分析

应急管理相关知识，建立统一的知识辅助分析功能模块。

4.1.4.3.4 情景智能方案

实现针对不同对象、不同阶段、不同灾害场景的多灾种灾害处置方案制定。

4.1.4.3.5 行政执法监察决策分析

通过对安全生产行政执法相关的大数据分析结果，发现事故隐患发生的规律性和

内在的关联性，找出安全监管工作的重点行业领域、地区、直至具体的企业名单，从而可以找出下一步安全监管执法工作的重点。

4.1.4.3.6 安全生产事故规律挖掘分析

根据安全生产内部数据和外部数据资源，对事故发生的关键节点进行建模。

4.1.4.3.7 应急资源保障情况分析

包括应急资源大数据图谱分析、危化品事故应急资源大数据图匹配、重大危险源事故应急资源大数据图匹配、非煤矿山事故应急资源大数据图匹配、工商贸其它事故应急资源大数据图匹配、山体滑坡灾害应急资源大数据图匹配、洪涝灾害应急资源大数据图匹配、森林火灾应急资源大数据图匹配。

4.1.4.3.8 应急救援预案制定情况分析

通过不同类型的预案内容、以及预案所针对的不同行业、不同级别、不同事故隐患进行分类汇总分析，包括应急救援预案大数据图谱分析、政府应急救援预案制定情况分析、企业应急救援预案制定情况分析、事故灾害前后应急预案对比分析。

4.1.4.3.9 隐患分布规律分析

根据对隐患排查各类属性的研究分析，选取所在地区、所属行业、隐患类型、隐患等级等作为统计维度组合时间维度，采用数据统计和图表分析，包括企业隐患分布规律分析、隐患地域分布规律分析、隐患时间分布规律分析、重大隐患分布预警、预警模型调整。

4.1.4.3.10 安全生产分析报告

提供报告指标维护功能，根据业务需求维护关注的业务数据指标支持模板维护和报告发布等功能。

4.1.4.3.11 互联网舆情分析

充分利用现有的舆情监测系统，将舆情监测数据通过网络爬虫等工具爬取的结构化数据、非结构化数据对接到安全生产大数据资源中心，进行分类存储。包括舆情采

集数据对接、数据目录梳理、数据词库、索引生成、公共突发紧急事件预警、专题信息大数据图分析、事件舆情分析。

4.1.4.4 决策优化系统

结合河南省应急管理实际需求汇聚，各类监测预警数据、监督管理数据、指挥救援数据等，结合大数据分析挖掘和人工智能进行辅助分析，进行灾害事故综合研判，并通过闭环反馈逐步进行决策优化，为领导提供辅助决策支撑。

4.1.4.4.1 建议报告优化

系统根据应急管理部根据日常工作内容，不断调整优化报告内容，让领导及时了解应急管理工作及重要信息。

4.1.4.4.2 监测预警优化

利用数据分析技术，匹配多种环境监测对象和监测参数，通过科学合理的组合布点，使得预警精准化、高效。

4.1.4.4.3 监督管理优化

监督管理主要从业务流程、业务内容、业务覆盖面等方面优化提升，辅助领导掌握监督管理工作整体情形，使得监管更精细、更科学。

4.1.4.4.4 指挥救援决策优化

为保障救援的高效、快速，急需要进行调整，实现对应急物资、救援力量的快速联系、指挥和调度，以科学化的处置方式优化调度策略及辅助方案。

4.1.4.4.5 安全投入规划决策分析

为生产经营单位的重点部位、重点场所加强安全管控、各项安全生产工作部署提供辅助决策依据。提供政府政策制定辅助决策参考指标、生产经营单位工作部署辅助决策参考指标。

4.1.4.4.6 应急救援指标体系分析

应急救援指标体系是建立在应急资源、应急预案、应急演练的建设基础之上，在事前进行管理和预防。

4.1.4.4.7 应急救援数学模型建模

应急救援的数学模型建设，需要对应急资源、应急预案、应急演练等一些因素指标的数量和关系上，进行计算和分析，需要在距离事发地点的一定范围内进行搜索和匹配。

4.1.4.4.8 应急救援指挥人员推介

筛选适合的相关人员清单，推荐给现场救援领导小组进行选取，以组成应急救援和指挥小组。

4.1.4.4.9 救援疏散路径分析

根据现场的道路交通情况，计算出从救援出发点到事故发生地点的多条救援路径。

4.1.4.4.10 协同救援电子标绘

根据不同的事故类型，为特殊的安全事故和高级别事故，提供特殊救援参考意见，将这些意见通过电子标绘的形式绘制在 GIS 地图界面上。

4.1.5 政务管理业务域

4.1.5.1 应急管理服务内网门户

应急管理服务内网门户建设主要包括门户网站栏目规划和门户管理功能两部分。一级栏目规划首页菜单栏、新闻发布、信息发布、统计报表、气象预警、应用超市 6 部分；门户管理功能主要包括栏目信息管理、信息发布、权限控制。

4.1.5.1.1 网站栏目规划

包括首页菜单栏、新闻发布功能区、消息发布功能区、统计报表功能、气象预警功能、应用超市功能。

4.1.5.1.2 应用集成门户管理功能

栏目信息管理系统、信息发布、权限控制等功能。

4.1.5.2 应急管理社会服务系统

应急管理社会服务系统是面向社会群众的互联网政府门户系统，作为应急管理对内展示资源的窗口，是所有数据、服务、应用的统一出口，是用户登录平台、访问数据和调用功能的唯一入口，为各类用户使用和共享平台资源提供一站式服务。

4.1.5.2.1 网站栏目规划

包括办事服务、政民互动、专题专栏、机关党建、安全论坛、经验交流、光荣榜、预警信息、应急科普、事故信息、报送信息采用量、微信公众号、微博、智能问答、全文搜索等栏目。

4.1.5.2.2 网站管理功能

提供用户管理功能、权限管理功能、安全管理、栏目信息管理、内容管理等功能。

4.1.5.2.3 业务应用功能

包括信息公开、公共服务、信息报送系统、信息检索系统、手机端应用、交流互动、无障碍浏览系统、系统日志管理系统、统计分析平台等。

4.1.5.2.4 外部接口功能

支持支持通信接口、支持接口标准规范、支持发布系统与应用系统接口、和 OA 系统接口、和综合业务平台接口

4.1.5.2.5 数据迁移

新建网站应将老版本网站数据迁入。在迁移的同时要进行数据清洗工作，去除冗余信息、规范信息格式、梳理信息基本元数据、按照新的网站栏目频道结构重新分类数据信息。

4.2 成品软件

4.2.1 支撑软件产品

支持对从简单到复杂的数据结构中的大量数据进行收集、集成和转换基础工具。

4.2.2 数据资源管理系统

数据资源管理系统建设，主要是围绕应急管理的业务需要，构建数据接入、数据处理、数据资源池、数据服务、数据应用等体系，提供数据资源支撑。

4.2.2.1 信息资源规划

应急管理信息资源规划需编制应急信息资源目录，通过整理比对形成应急管理信息资源目录体系。包括信息资源的分类、元数据描述、代码规划和目录编制，以及相关工作的组织、流程、要求等方面的内容。通过建设信息资源目录体系，明确河南省应急管理厅信息资源的本质、范围、管理要求和共享要求，实现对信息资源的组织、存储、查找和定位；以信息资源交换、共享和查找利用为基本目标，实现信息资源物理分散、逻辑集中。

应急管理信息资源规划需编制应急信息资源目录，通过整理比对形成应急管理信息资源目录体系。包括信息资源的分类、元数据描述、代码规划和目录编制，以及相关工作的组织、流程、要求等方面的内容。

4.2.2.2 数据整合汇聚

数据整合汇集范围主要包括内部系统数据、其他部门共享数据、社会及互联网数据。

4.2.2.2.1 内部系统数据

内部系统数据汇聚，包括风险分级管控信息、隐患治理信息、非煤矿山、危化、烟花爆竹、安全生产规章制度、规程、安全生产标准化、安全评价情况、应急管理、应急救援等数据。

4.2.2.2.2 其他部门共享数据

汇聚成员单位数据。安全生产涉及范围广，牵扯单位多，数据资源管理系统需要采集相关的安委会成员单位数据进行统一分析。

4.2.2.3 应急管理数据资源池建设

应急管理数据资源池建设主要是针对整合接入的数据资源和应急管理厅采集汇聚的数据资源进行统一管理，通过构建原始库、资源库、专题库、主题库和配置库，构建一体化的数据资源支撑体系，为智慧应急信息系统建设提供数据资源保障。

4.2.2.3.1 原始库创建

通过数据接入系统引入抽取整合政务各委办局共享数据、感知数据、互联网数据、社会数据等实体数据形成。

4.2.2.3.2 资源库

资源库数据是对原始库数据进行提炼加工后形成的公共数据集合，对各项业务需求都具有支撑作用。应该包括监督管理类数据、监测预警类数据、指挥救援类数据、决策支持类数据和政务管理类数据。资源库的设计包括数据结构设计、数据表结构设计和加工过程设计。

4.2.2.3.3 主题库

主题库依据应急管理业务需求进行数据主题分类，基于面向对象的数据组织原则，以资源库为数据源，围绕某一主题对象进行数据分析和整理后形成数据集合。主题库根据应急管理业务，围绕灾害事故、管理对象、应急环境、救灾资源、动态感知等实体构建沉淀的一组数据建模方法和一系列基础算法从庞大的资源库中抽取共性的维度进行分析，形成高通用、易扩展和易使用的数据模型。

4.2.2.3.4 专题库

应急管理厅的业务主要包括重特大自然灾害和事故灾难的应急处置和工矿商贸等行业的安全生产监督检查等。我们按照常态、非常态相结合，偏重非常态的思路设计

专题库。

根据重特大突发事件的类型，本期将专题库划分森林火灾专题库、危化品事故专题库、煤矿事故专题库、气象灾害专题库、水旱灾害、地质灾害、火灾事故专题库，共计 7 个专题库。

4.2.2.3.5 配置库

配置库实现对数据治理系统中的各项过程进行记录与管理支撑，具体包括内容性与操作性方面的存储设计。

从配置内容来说，主要包括配置索引、配置知识、配置标签规则、配置日志管理等。从库表建设与存储设计来说，主要包括索引库设计、标签规则库设计、日志库设计及相关配置等。

4.2.2.4 数据治理系统

数据治理系统基于应急信息资源规划标准规范，利用数据接入、数据处理、数据管控、数据服务、数据共享交换等，完成应急管理体系内部、外厅局数据、企业感知数据的接入、处理、管控、共享和对外服务，形成统一的数据资源池，通过数据有效、合理、清晰、先进的架构设计实现应急管理数据资源的汇聚融合，提升价值密度，为上层业务系统提供高效的数据服务。

4.2.2.4.1 数据接入系统

数据接入系统主要实现应急管理业务所需源数据的统一接入，支持应急管理内部数据、外部厅局数据、社会及互联网数据、感知数据等全域应急数据的引接，涵盖监督管理、风险监测、指挥救援、政务管理等全业务域。系统能够实现数据探查、数据读取、数据对账、断点续传、任务管理、解压解密、数据分发等功能，通过统一接入，将源数据集中存储至原始库。

4.2.2.4.2 数据处理系统

数据处理系统通过采用自然语言处理、语音分析、生物特征识别等人工智能技术，

使用数据抽取、数据转换、数据清洗、数据关联、数据去重、数据补全、数据关联、数据融合、数据比对、数据标识等规范化数据处理手段处理各类数据，为构建数据资源池提供支撑。

4.2.2.4.3 数据资源管理

按照应急管理业务需要，通过多种维度直观的展示当前汇集的数据种类、数据量、数据来源、数据每日增量等情况，为掌握当前数据情况提供可视化的参考标准。

4.2.2.4.4 数据质量管理

建立数据质量评估标准和管理规范，提供数据质量问题发现、监测跟踪、分析应用等闭环流程和管理功能，实现基于不同来源数据的逻辑校验和监测管理；实现数据源头采集、传输、应用全流程的规范性、一致性、准确性、完整性检查；实现数据质量问题监测预警，支持监测预警规则动态调整。数据质量管理包括数据标准管理、元数据管理、质量指标、质量报告、质量点监测、数据分析、数据指标管理、脚本监测、数据脱敏管理、数据价值评估。

4.2.2.4.5 数据安全

数据安全包括数据安全加密传输、数据交换过程的安全保障、数据交换接口安全设计、数据审计与防护。

4.2.2.4.6 数据监控管理

应急管理数据资产进行统一的管控，实现数据运维管理、数据血缘管理、数据分级分类、数据运营管理、数据资产管理、数据资源监测、数据集成系统监控、数据服务体系监控、数据入库监控、数据库运行监控、服务调用监控等主要功能，开展统一的数据全生命周期管理服务，规范数据环境，提高数据质量。

4.2.2.4.7 数据治理可视化

利用可视分析引擎对各类应急数据资源进行主题分析，可视化分析引擎的图形化分析手段表达信息资源分析逻辑，自助式构建数据治理可视化分析和业务资源可视化

分析，满足信息资源简洁、高效、灵活及多元化的可视化展示要求。包括多数据质量可视化分析、多数据接入可视化分析、多数据处理可视化分析、数据管控可视化分析、数据应用情况可视化分析。

4.2.2.5 数据服务系统

数据服务系统提供分类建设的多渠道、多维度的数据服务模式，面向基层用户提供查询检索、数据比对、数据订阅等基础数据服务，所有的服务统一注册平台 API 网关，通过统一鉴权实现对外开放共享。

4.2.2.5.1 数据服务开放平台

数据服务平台是数据服务系统核心组成，为各业务部门提供标准化、共享的、安全的数据资源服务，实现中心数据资源对外统一服务、资源共享与管理，从信息资源共享服务的角度出发实现横纵向的互联互通。资源服务总线主要包括服务注册、服务发布审批、更新服务、删除服务、发布服务草稿、服务禁用\启用、流量控制配置、负载均衡、流量控制、超时配置。

4.2.2.5.2 数据服务目录

数据服务目录包括数据目录发布、数据目录审核、数据目录服务、专题数据服务、查询检索服务、数据获取服务、数据鉴权服务、数据接口服务。

4.2.2.5.3 资源服务反馈

资源反馈，为服务开放平台开发者对数据资源的申请、评价、纠错等信息提供展示及处理功能。

4.2.2.6 数据应用建设

数据应用建设包括主数据管理、应急管理一张图、数据共享。

4.2.2.6.1 主数据管理

主数据管理包括数据勘误、数据补录、数据合并、数据拆分、数据日志。

4.2.2.6.2 应急管理一张图

整合应急数据资源，包括应急机构、应急物资、救援队伍、应急专家、防护目标等信息，在 GIS 地图上进行统一标注。“应急管理一张图”可实现应急相关数据的存储、检索和管理功能，系统可进行“分级分权”设置，功能包括图层筛选、特定目标查询、风险信息一张图、重大危险源一张图、区域风险态势一张图、隐患信息一张图、应急资源一张图、应急救援一张图。

4.2.2.6.3 数据共享

遵循部级数据共享交换标准开展本地数据共享交换系统的建设。数据共享交换功能通过库表、文件、服务接口等方式实现地方应急管理部门内部以及与外部的数据共享交换。主要功能包括对外信息采集系统、前置机系统、交换管理系统、信息资源发布、信息资源订阅、数据交换服务、数据共享查询、对外数据共享。

4.2.3 应用支撑系统

应用支撑平台提供应用界面设计规范，并以通用应用支撑模块提供用户管理、单点登录、权限管理等功能，实现对各业务系统门户的风格统一和单点登录的功能。通用应用支撑为整个平台提供了应用开发环境、应用集成环境、系统运行保障等公共应用服务。应用支撑中的服务是由可插拔的组件封装而成的标准服务，可以供各业务系统直接调用，既能为新建应用开发提供支撑服务，也可以用于构建应用整合服务，为已建成的、第三方的应用系统提供整合支撑服务。

应用支撑平台建设主要包括基础支撑软件、移动服务平台、服务开放系统、系统对接整合等建设内容。

4.2.3.1 基础支撑软件

为信息系统的规划、设计、开发及运行维护提供统一的标准规范和架构，平台提供统一管理展示用户信息、组织机构、业务应用系统运行情况，并提供访问排名、访问数量、登陆情况、用户数等，平台包括统一用户、统一授权、统一认证、统一审计

等功能，为上层业务应用系统提供基础配置类微服务组件，用以实现业务流程定制、整合。

4.2.3.1.1 统一地理信息服务

根据应急管理 EGIS（应急管理地理信息云平台）建设要求，调用 EGIS 图层，结合本次建设业务图层需求形成河南省应急管理统一地理信息服务，并对各种基础性的地理信息二次开发组件进行封装，统一提供服务。

4.2.3.1.2 模型支撑

充分利用部里建设的模型工厂，形成算法模型承载环境及基础算法模型库，为应急业务提供智能化模型服务，结合自身业务需求，开发基于业务场景的模型。

4.2.3.1.3 算法支撑

充分利用部里建设的模型工厂，构建了算法管理、算法开发、业务模型开发等能力，结合自身业务需求，开发基于业务场景的算法。

4.2.3.1.4 统一用户

包括组织机构管理、部门配置管理、用户配置管理、岗位职务管理、用户组管理功能，对组织机构和用户进行统一管理，将组织机构和用户信息通过接口供业务应用系统调用，实现对组织机构和用户信息的分级管理和同步更新，提高组织机构和用户数据的管理、展现、前台调用的灵活性、便捷性。

4.2.3.1.5 统一授权

实现对业务应用系统权限的统一管理，支持基于 RBAC 的授权管理机制和基于 PMI 的权限管理模式，对业务应用系统提供顶层权限管理模式、系统功能权限管理模式，也可提供两种权限管理模式的叠加应用。包括业务应用系统权限注册、多级分层授权、精确授权和复制授权、授权审批、审计和日志管理功能。

4.2.3.1.6 统一认证

包括用户身份认证、会话管理、证书管理、策略管理等功能，实现用户身份的统

一校验，为业务应用系统提供单点登录服务。

4.2.3.1.7 统一门户

统一门户是厅内信息系统统一入口，基于平台统一的安全认证体系，一次登录，全网漫游，为用户提供应用系统快捷入口，面向应急管理各级各类用户，提供统一的门户服务。主要功能包括门户管理、微件管理、内容管理。

4.2.3.1.8 统一 workflow

统一 workflow 微服务组件实现流程服务自定义、workflow 引擎、流程服务列表、统计服务、模版管理等功能，提供具有安全、可靠、稳定、可灵活应用的 workflow 引擎，支持流程的顺序、并行、选择和重复执行等方式，实现各种流程的图形化配置。

4.2.3.1.9 统一表单

统一表单微服务组件为业务应用系统提供不同种类界面要素、流转单据的定制及展现，通过统一表单引擎中的表单设计器，以图形化拖拽的方式快速定义各类表单要素。

采用统一表单微服务组件，该组件包含一个完整的表单设计器，主要功能包括表单样式可视化设计、搜索及高级搜索、自定义展现标签、自定义排序、自定义展现字段、历史变更记录、可视化操作。

4.2.3.1.10 统一消息

统一消息微服务组件提供站内消息、短信、站外邮件、消息盒子等功能，通过服务接口实现与业务应用系统的消息、任务的汇聚与分发，将业务应用系统的任务和消息信息传送给用户。

4.2.3.1.11 统一文件

提供统一的附件管理功能，可在线查看附件存储目录，和每个目录的实际存储情况等信息。提供文件上传、文件下载与浏览、文件管理维护、网盘管理、文件提取等功能。

4.2.3.1.12 设置中心

设置中心就相对公共的基础设置类组件进行统一管理，参数中心、图标管理、状态机管理、字典管理、工作组管理、部署信息、意见管理、流水号管理、数据权限管理、证照管理、打印管理等公共的部分进行统一的管理，统一入口。

4.2.3.1.13 缓存中心

缓存中心对热点数据缓存，提高业务系统性能，供平台、业务应用直接调取使用。

4.2.3.1.14 任务调度中心

任务调度中心实现对任务的统一管理、统一调度，合理分配系统各任务的运行时间，支持各系统自行注册任务。功能主要包括：调度策略配置、分布式任务调度、调度记录、调度任务监控。

4.2.3.1.15 运维监控中心

需要随时监控系统各个部分的运行状态、根据各部分运行状态及时找出问题和瓶颈并加以解决。其功能主要包括：系统运行监控功能、用户登录情况监控、应用系统的运行状态监控。

4.2.3.2 移动服务支撑

当前应急厅面临复杂的移动应用场景：已建成多个 APP，未来还有其他业务系统 APP 要开发上线，但各个 APP 之间存在数据烟囱和信息孤岛的情况。账号不统一，版本各自升级，开发模式也各不相同，有原生开发、有 HTML5 开发还有 webAPP，因此导致移动端存在巨大的管理困难。针对上述情况，移动服务平台提供一整套解决方案，包括一个强大的 APP 门户和管理平台。

4.2.3.2.1 移动应用中心

移动应用中心功能包括应用注册、版本管理、应用监控。

4.2.3.2.2 移动安全中心

移动安全中心功能包括设备管理、用户授权、认证管理、用户审计。

4.2.3.2.3 移动接口中心

为了实现信息稳定、可靠的传输，屏蔽掉因业务端协议、参数、返回值等繁琐的适配转换工作，为移动端开发提供一个统一、标准的信息通道，功能包括接口注册、接口管理、接口测试。

4.2.3.2.4 移动服务中心

移动服务中心功能包括统一消息中心、统一任务中心、统一缓存中心、基础功能服务。

4.2.3.2.5 移动统计分析

通过用户行为数据对应用和终端的使用情况进行详细地分析汇总，提供用户统计、应用统计、接口统计等多种统计维度。

4.2.3.2.6 移动 APP 集成服务

移动 APP 集成服务包括集成门户、应用定制功能。对所有已集成的 APP 应用，实现统一登录认证和集中展示，对当前登录用户权限范围内的移动 APP 可进行定制，设定在移动集成门户显示与否以及显示位置。

4.2.3.3 服务开放系统

服务开放系统采用微服务架构，由三类服务、一种服务开放体系构成其中分布式架构又分为分布式服务框架与分布式部署架构，在分布式服务框架中包括了服务引擎、服务路由、负载均衡等内容。

4.2.3.3.1 开发者中心

开发者中心，为开发者提供注册，系统文档浏览等功能，为管理者提供开发者账号管理、系统文档管理、维护与发布。

4.2.3.3.2 应用中心

应用中心，为开发者提供应用的接入、应用密钥的申请、重置（在密钥泄露时），为管理者提供应用的审核、上下线管理、密钥授权的功能。主要包括创建应用、上线

审核、版本列表、我的应用、应用列表等功能。

4.2.3.3.3 服务中心

服务中心，为开发者提供服务的接入、服务的申请、在服务实例有多个实例时，为服务提供负载均衡，并为管理者提供对服务的审核、授权、管理监控功能。主要功能包括微服务管理中心、微服务网关、服务目录、服务开放、服务编排、服务引擎、协议适配、事务管理、服务安全、缓存中心、开放应用支持体系、应用系统接入。

4.2.3.4 系统对接整合

为适应河南省应急管理厅机构改革及业务的调整，满足对多部门、多应用的统一集中管理、使用的需求，对已经在使用的河南省应急管理综合业务平台进行全面再造升级，以实现在 PC 端进行系统统一登陆、统一待办处理、数据共享。

同时，为满足对多部门、多移动应用的统一集中管理、使用的需求，对已经在使用的河南省应急管理综合业务平台提供的移动 APP 进行全面再造升级，以实现在 HTML5 框架协议下的接口统一调用。

4.2.3.4.1 业务数据共享

结合河南省各应急业务相关系统现状，将分散、异构的业务应用和信息资源进行整合，通过数据共享交换系统与上下级平台以及其他部门业务系统实现数据交换，上下级平台及横向部门业务数据的集成。包括风险点基本信息共享、公安机构信息共享、事故信息共享、危化品信息共享、应急救援队伍信息共享、应急物资装备信息共享、应急预案信息共享、专家信息共享等。

4.2.3.4.2 系统单点登录集成

范围包括企业数据中心系统单点登录、行政许可系统单点登录、行政执法系统单点登录、风险管控系统单点登录、隐患排查治理系统单点登录、业务知识库系统单点登录、重大危险源系统单点登录、综合展现门户系统单点登录

4.2.3.4.3 待办业务统一处理

范围包括危险化学品安全生产许可证(省级)待办统一处理、危险化学品经营许可证（市级）待办统一处理、危险化学品经营许可证（区县级）待办统一处理、危险化学品安全使用许可证待办统一处理、危险化学品安全生产许可证(市级)待办统一处理、烟花爆竹生产企业安全生产许可证（省级）待办统一处理、烟花爆竹经营（批发）许可证（省级）待办统一处理、烟花爆竹经营（批发）许可证（市级）待办统一处理、烟花爆竹经营（零售）许可证（区县级）待办统一处理、非煤矿山企业安全生产许可证（省级）待办统一处理、非煤矿山企业安全生产许可证（市级）待办统一处理、非药品易制毒化学品（第一类）生产许可待办统一处理、非药品易制毒化学品（第一类）经营许可待办统一处理、非药品易制毒化学品（第三类）经营备案待办统一处理、安全生产检测检验机构资质认可待办统一处理、安全评价机构资质认可待办统一处理、生产安全事故应急预案备案待办统一处理、危险化学品重大危险源备案待办统一处理、非煤矿山建设项目安全设施设计审查待办统一处理、危险化学品建设项目安全设施设计审查待办统一处理、金属冶炼建设项目安全设施设计审查待办统一处理、危险化学品建设项目安全条件审查待办统一处理。

4.2.3.4.4 移动 APP 集成

将河南省应急管理综合业务平台政府端 APP 按当前原生方式整包集成到移动服务平台，并将河南省应急管理综合业务平台政府端 APP 与移动服务平台进行单点登录集成。

4.3 安全产品

4.3.1 防火墙

1U 机型，单电源，三层吞吐量 5G，并发连接数：260 万，集成访问控制、应用层威胁防护等一系列网络安全功能，满足虚拟化云环境在云边界的安全域隔离、访问控制、威胁防护、失陷检测和安全管理等需求系统；三年硬件保修和技术支持服务。

4.3.2 主机安全加固

提供 50 个虚拟化主机安全代理防护能力，集主机防火墙、主机入侵防御、Hypervieor 层防护、主机加固、webshell 检测于一体，支持 Windows2008 R2 X64 、Windows2012 R2 X64 或 Linux 上部署。

4.3.3 防病毒

提供 50 个虚拟主机杀毒能力，有效查杀主机上的文件、内存、进程中的恶意程序，对主机进行统一的病毒查杀管理，制定定时查杀任务，辅以主动防护引擎和文件监控

4.3.4 数据库审计

2U，提供数据库操作行为审计、事件追踪、威胁分析、实时告警等多种功能，三年硬件保修和技术支持服务。

4.3.5 数据库防火墙

2U，多因子认证、屏蔽直接访问数据库的通道、攻击检测和保护、连接监控、虚拟补丁、报表、安全审计，三年硬件保修和技术支持服务。

4.3.6 网页防篡改

对 Web 站点目录提供全方位的保护，防止黑客、病毒等对目录中的网页、电子文档、图片等任何类型的文件进行非法篡改和破坏

4.3.7 Web 应用防火墙

1U 机型，单电源，三层吞吐量 3G，http 并发连结数 20W，保证 Web 应用合法流量的正常传输，保障业务系统的运行连续性和完整性。实时拦截各种 WEB 攻击，能有效拦截各种 SQL 注入，XSS 跨站类型的 WEB 攻击。

4.3.8 堡垒机

1U 设备，单电源，包含 50 台设备资产安全配置检查和变更检查授权，三年硬件保修和技术支持服务。

4.3.9 漏洞扫描

1U 设备，单电源，最大并发扫描 50 个，提供资产管理、系统漏扫、网站漏扫、数据库漏扫、基线配置核查、弱口令扫描等功能。三年硬件保修和技术支持服务。

4.3.10 日志审计

1U 设备，单电源，含 50 个主机审计许可证书，处理性能 3000 条/秒，三年硬件保修和技术支持服务。

4.3.11 安全管理中心

响应中心：提供安全摘要报表、主机威胁报表、脆弱性分析报表、报表个性化订阅、安全设备联动配置与管理等能力。

智能安全分析：可检测如 webshell 后门、黑链、勒索行为、慢速扫描等，相比规则类检测，机器学习可以提高检测的准确率。

通报预警：包括安全告警、处置工单、统计分析、工单处理流程管理、工单编辑等。

智能安全分析：可检测如 webshell 后门、黑链、勒索行为、慢速扫描等，相比规则类检测，机器学习可以提高检测的准确率。

通报预警：包括安全告警、处置工单、统计分析、工单处理流程管理、工单编辑等。

日志审计/检索：可检索、查看、审计安全日志、操作记录、FLOW 形式的数据源等。

综合管理：对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。”

4.4 标准规范

依据国务院印发的《“十三五”国家信息化规划》和国务院办公厅印发的《“互联网+政务服务”技术体系建设指南》，设计支撑应急管理数据标准化的应急管理数据规范。依据国标、行业标准及应急管理部制定并下发的相关信息化标准，结合河南省安全监管平台建设实际需求，梳理应用系统建设、信息资源标准、数据共享标准、系统接口规范等标准规范内容，通过标准化的操作指南，实现应急管理的标准化、流程化实施。

序号	类别	梳理项目
1	应用系统建设	系统开发规范
		文件编制规范
		软件管理规范
2	信息资源标准	分类与编码规范
		信息模型
		数据项和值域范围
		数据质量规范
3	数据共享标准	数据交换格式
		数据发布规范
		共享系统运行规范
4	系统接口规范	系统接口标准编写规范
		感知数据交换规范
		视频监控联网技术要求

4.5 系统对接

根据应急管理部以及河南省人民政府相关要求，在项目建设期内，平台按需提供标准接口与河南省“互联网+监管”系统、河南省政务服务网及其他相关系统平台实现数据共享与业务协同。

五、应用系统技术指标

指标项	系统	指标要求
监督管理业务域	行政许可四级十同	实现省政务服务平台、省在线审批平台的集成与数据回流。
	行政执法系统	对离线状态下登记的执法检查记录和企业隐患信息进行上传。
	安全生产培训考试系统	安全生产考试子系统提供与河南政务服务网数据同步接口、EMS 邮寄接口、短信接口、支付接口、与实操模拟设备之间

		接口、地图接口。
	双重预防体系系统	安全生产双体系系统支持对风险、隐患的闭环管理
监测预警业务域	三维可视化监管	选取 4 个试点企业进行框架式的人工建模，其中包括厂房内主要基础设施设施的适应性建模，重点监管对象和场景的真实模拟。
	安全生产风险评估系统	构建风险监测指标体系和风险评估模型，利用大数据、人工智能等技术手段，针对特定区域、事故进行风险评估。
	自然灾害监测预警系统	接入利用其他行业部门部分灾害预警数据、历史灾害数据、自然灾害背景信息、基础背景空间数据等，实现气象、洪涝、地震等自然灾害的监测预警及统计，并实现对特定范围目标的预警信息精准推送，形成预警信息数据一张图可视化。
指挥救援业务域	应急指挥信息系统	围绕贯穿全流程的值班值守等业务，事发、事中、事后各阶段的业务，构建指挥救援全流程业务功能。
	结构化预案管理系统	实现应急预案编制流程的信息化处理、预案数字化处理、各级各类应急预案的多维查询和基于图表的统计分析。
	应急资源管理系统	实现救援物资普查功能，对全省应急基础数据的统一管理，提供基础数据的多维查询及基于图表的统计分析及空间分布。
	专题研判系统	充分利用大数据挖掘分析技术，通过多灾种耦合及次生、衍生灾害演化模拟模型，实现事故灾害发展趋势分析、事故影响后果分析、次生衍生灾害分析、灾情损失评估等功能。
决策支持业务域	智能云搜系统	运用先进的云计算、大数据挖掘、统计分析技术，实现对海量应急数据的关联查询，系统以数据资源管理系统汇聚的海量数据为基础，通过关键词提取、NLP 自然语言分析与映射等，实现对相关业务信息快捷、即时、多维度的查询展现并根据业务属性建立全息企业档案及应用。
	态势感知系统	基于大数据分析及人工智能技术，针对风险数据、监测数据、预警数据、灾害数据、事故数据、舆情数据深入分析，实现态势感知展示当前态势的演化趋势。
	辅助分析系统	利用多源数据融合技术下的灾害数据深度挖掘分析、大数据可视化表达等技术，分析已有案例推演情景形成的灾变演化场景规律提出风险防护、处置救援、资源调配建议，为事故救援处置提供辅助决策支撑。
	决策优化系统	常态下通过自然灾害、安全生产、综合防范的各类风险评估、监督管理结果的统计分析、灾害事故指挥救援的总结评估，形成对监测预警、监督管理、指挥救援、政务管理各个环节的闭环反馈与优化，非常态下通过实时监测数据、事件续报信息、事件态势研判分析对模型参数进行优化，完善决策方案优化决策结果。
政务管理业务域	应急管理服务内	应用集成门户的栏目可以方便定制，而且栏目在首页面上的

	网门户	位置可以进行灵活的调整。支持整站、栏目组克隆功能，提升建设效率。支持新增多栏目合并功能，使结构调整更加方便、快捷。支持多种栏目发布方式设置，实现及时、定时、手工发布方式。
	应急管理社会服务系统	实现对网站内容管理，支持可视化的内容编辑器，充分实现图文混排功能。

六、成品软件技术指标

下述技术参数要求中加“▲”标志的为重要响应指标，其余的为一般响应指标。

1、数据资源管理系统技术指标

指标项	指标要求
数据接入	统一的数据采集接入方式，支持多种类型的数据源，包括但不限于 Oracle、MySQL、SQLServer、DB2、瀚高等国内外主流关系型数据库；HBase、MongoDB 等 NoSQL 数据源等（要求提供软件功能截图证明材料）
	适配各种主流大数据平台，包括但不限于 Hadoop、Hive、HBase、MaxCompute 等
	支持数据库基于日志实时增量数据抽取，包括但不限于 Oracle、MySQL 等。
	支持用户管理，自定义角色权限，支持白名单管理（要求提供软件功能截图证明材料）
	具备丰富的 ETL 组件库，可实现数据抽取、关联、排序、去重、转换、聚合、装载等功能
	提供软件著作权证明材料
数据处理	支持通过图形化的拖拽方式，将不同类型节点连线组织开发成工作流，便于用户自主管理作业的部署以及生产监控运维（要求提供软件功能截图证明材料）
	支持工作流的导入导出操作，包括但不限于工作流、自定义函数、资源文件和模型等，便于离线备份和异地发布（要求提供软件功能截图证明材料）
	提供可视化的数据清洗转换组件，通过托拉拽操作实现过滤、清洗转换功能。数据过滤支持组件包括但不限于长度过滤、正则过滤、标准值域过滤、空值过滤、相等过滤、比较过滤等；

指标项	指标要求
	<p>质量组件包括但不限于去除特定字符、大小写转换、数据脱敏、汉语转拼音、字典标准化和身份证校验转换等</p> <p>▲提供软件著作权证明材料</p>
数据监控管理	<p>支持全链路数据血缘分析和展示，用户可以根据数据库血缘清晰的查看数据在数据源之间的总体流向，支持库级、表级、字段级血缘分析，可以基于血缘信息进行溯源分析和影响分析（要求提供软件功能截图证明材料）</p> <p>提供软件著作权证明材料</p>
数据服务目录	<p>支持目录批量导入和导出功能（要求提供软件功能截图证明材料）</p> <p>提供资源发布、资源申请、资源供应流程的自定义修改功能（要求提供软件功能截图证明材料）</p> <p>目录发布阶段，审批方式支持部门内自行审批和上级部门集中审批两种审批模式（要求提供软件功能截图证明材料）</p> <p>一个目录支持关联多种资源类型，包括库表、接口、文件。（要求提供软件功能截图证明材料）</p> <p>支持按照数据来源、主题库和专题库等维度来进行信息资源的类目划分</p> <p>提供软件著作权证明材料</p>
应急管理一张图	<p>可实现应急相关数据的存储、检索和管理功能，系统可进行“分级分权”设置，功能包括图层筛选、特定目标查询、风险信息一张图、重大危险源一张图、区域风险态势一张图、隐患信息一张图、应急资源一张图、应急救援一张图</p> <p>提供软件著作权证明材料</p>
主数据管理	<p>支持数据勘误、数据补录、数据合并、数据拆分、数据日志</p> <p>提供软件著作权证明材料</p>
国产化/扩展性要求	<p>支持国产化硬件产品的适配，如服务器、客户端、CPU、操作系统、中间件、浏览器等。</p> <p>▲提供软件著作权证明材料。</p>
高性能、高可靠	<p>▲提供相应软件的测试报告，测试报告的出具单位须为中国合格评定国家认可委员会所认证的认证机构或实验室。测试报告至少覆盖数据相关的三个模块：数据交换、数据治理、数据集成，其中关键指标满足不低于 200 并发时，</p>

指标项	指标要求
	响应时间不得超过 2 秒。
	▲应满足省市县三级系统高效稳定运行，支持单集群大规模滚动升级与补丁能力，业务不中断，一次升级少量节点，循环滚动，直至集群所有节点升级到新版本，能支持不少于 500 节点和 10PB 级数据量的滚动升级，并提供相关证明材料。

2、应用支撑系统技术指标

指标项	指标要求
统一地理信息服务	支持多种 GIS、建模工具
	采用配置式选择设置，叠加数据图层，实现 GIS 应用快速构建
	支持数据制图、图层管理、符号化设置及专题图输出
模型支撑	提供从数据准备、模型开发和训练、模型评估、模型部署到在线推理的端到端数据智能；
	集成丰富的自然语言处理和理解组件，轻松实现非结构化文本的预处理，你可以结合机器学习随心所欲对文本数据进行分析、探索和理解；
	集成 Spark ML，支持分布式机器学习
	提供众包数据标注工具，支持多种标注类型任务的创建、标注、审核以及验收能力
	支持自动化机器学习，为无开发能力的业务开发者，实现零基础构建 AI 模型
算法支撑	支持内置词库，涵盖自然科学、工程科学、社会科学、学术术语、地名、机构名、人名以及法律、金融、财经、电商、教育、通信、旅游、时政、交通运输、互联网等近百个领域/行业；
	提供标准化的 RESTful API 和 SDK，方便用户开发调用；
	基于丰富的算法模型，高效挖掘文本价值；
	支持敏感词识别，帮助客户识别涉政，涉黄，涉暴，垃圾广告等违规单词，从而提供安全保障；
	提供分词词性标注能力，对输入的连续的自然语言文本切分成具有语义合理性和完整性的词汇序列，并为每个词汇赋予一个词性；
	支持关键词提取，从文本中提取出有代表性的关键词，帮助人们从海量数据中自动获取关键信息

指标项	指标要求
统一用户	支持用户管理、组织机构管理、部门配置管理、用户配置管理、群组信息管理、用户注册流程、用户变更流程、用户注销流程等功能，对组织机构和用户进行统一管理，将组织机构和用户信息通过接口供业务系统调用，实现对组织机构和用户信息的分级管理和同步更新。
	支持基于 LDAP 的组织机构用户同步功能，平台将用户信息推到 LDAP，第三方从 LDAP 服务器获取（要求提供软件功能截图证明材料）。
	支持基于 RabbitMQ 的组织、用户、角色的同步和消息订阅。
	提供软件著作权证明材料。
统一认证	支持 OAuth2、CAS、keycloak 等多种认证方式。
	支持通过多种手段保证票据（Ticket）的安全性，保证票据不可被仿造。从而防止非法用户的侵犯，保证合法用户单点登录、全网漫游。
	支持 IP 地址控制策略、会话有效期策略、登录次数策略、是否重复登录策略、审计策略，数据备份策略等；
	支持提供 redis 会话数据的存储、分配会话标识,并通过使用 cookie 或 URL 重写来跟踪与每个客户端请求相关的会话标识；
	提供软件著作权证明材料。
统一授权	支持应用权限注册、多级分层授权、精确授权、复制授权、授权审批、访问控制等功能,实现对业务应用系统权限的统一管理。
	支持基于 RBAC 的授权管理机制和基于 PMI 的权限管理模式。
	对业务应用系统提供顶层权限管理模式、系统功能权限管理模式、数据权限管理模式。
统一审计	支持提供标准接口整合已有业务应用系统的审计信息；
	高级查询支持系统名称、模块名称，关键字(如用户名、组织名、IP 以及生成的时间段等信息)等进行组合查询及逐层查询；
	支持基于固定的日志格式对系统运行情况进行性能分析和用户行为的全链分析。
	支持基于图形化的日志分析工具，实现审计数据采集、管理、可视化的统一审计体系。
统一门户	支持通过多维度导航、信息聚合、动态推介等方式,将热点关注和重点推荐的内容突出；
	支持依托内容管理工具为管理员用户、业务人员用户按照权限实现群组、个人工作界面的构建，至少包括统一视图、个性化定制、应用整合，业务协同，安全控制等功能；
	提供软件著作权证明材料。
统一 workflow	支持流程基本属性定义、流程环节定义、角色权限设置、流程路由定义、流程高级定义、图形化流程设计、workflow 管理及监控、workflow 建模等功能

指标项	指标要求
	提供图形化方式辅助业务人员建模,图形化的过程模型采用活动网络图、支持减少组成模型的元素,分离数据流逻辑和控制流逻辑;
	支持控制表单中的某些元素和功能实现定义流程,通过建立表单元素控制表来输入包括界面元素、功能元素等;
	支持 WFMC 国际标准、支持并行、串行、环形拓扑结构;
	提供软件著作权证明材料。
统一表单	支持表单定义以所见即所得的方式定制报表的存储结构和录入界面的布局、样式等;
	支持将定义的报表,审核,汇总等基于 XML 的描述文件编译生成为可执行的数据录入、查询、汇总界面;
	支持对表单上的字段进行绑定操作,设置各类控件,如下拉框、单选框、多选框、文本框,富文本、关键字、附件、按钮等,同时支持根据定义的字段直接创建数据库表或字段
	支持通过中介媒体来实现交互,与统一工作流微服务组件的捆绑;
	提供软件著作权证明材料。
统一消息	支持统一的即时通讯工具,当用户登录即时通讯工具时,支持即时提醒业务应用系统中的待办任务和邮箱中的未读邮件;
	统一的消息,任务的汇聚与分发中心,通过服务接口接收应用系统的任务和消息信息;
	支持多种消息处理的业务应用系统接口,包括邮件提醒、即时消息提醒、任务提醒等;
	支持集中的任务中心,任务中心收集各个业务系统的待办任务,通过门户系统来展现,任务中心自动调用消息中心的接口,给业务人员发送任务提醒消息。
统一文件	提供统一的附件读取、写入接口,支持业务系统进行附件读写
	支持在线查看附件存储目录和每个目录的实际存储情况
	支持对个人网盘默认大小、上传附件大小进行全局默认设置
	支持批量对多个文件或文件夹进行打包下载、移动、删除操作
	支持多种存储方式的扩展,包括本地存储、HDFS 分布式存储、Hbase 存储、Swift 存储
设置中心	支持针对全局、一级应用、二级应用、实例四个级别设置参数
	支持自定义图标并提供通用的地址供开发人员使用
	支持字典管理,对外暴露 API 接口和通用帮助页面,方便其他应用使用

指标项	指标要求
	支持流水号管理，简单、灵活的规则配置，方便的 API 接口和通用帮助页面
缓存中心	支持本地缓存和远程缓存，远程缓存又包括 Redis 和 EhCache 等多种方式
任务调度中心	支持图表的形式展示每天的任务及调度情况
	支持可视化任务管理界面
	支持任务的调度情况查询
	支持异步调度，提高性能
	完善的使用教程，方便户快速熟悉使用
运维监控中心	支持监控 k8s、nginx、数据库（oracle、mysql 等数据库）、服务器的相关指标
	支持根据 prometheus 相关告警语句制定相关的告警规则，产生相关的告警信息，通过邮件系统推送到线管人员。
	支持根据告警规则添加监听人员，产生告警信息时推送相关人员
	提供软件著作权证明材料。
移动服务支撑	支持已建、在建、新建应用 APP 集成支撑
	支持安卓原生以及 H5 或者两者混合作为技术架构的 APP 集成
	提供软件著作权证明材料。
服务开放系统	支持多级部署，敏捷支持灵活多变业务，一站式解决应用、服务的发布、交付和维护问题。
	以云原生为基座支持分钟级应用实例快速拉起。
	提供统一应用生态管理工具，支持链接挂载、Helm 模板、二进制文件包、在线设计（webStudio）等应用入驻方式
	提供统一服务生态管理工具，支持接入组件服务、AI 服务、数据服务等各类 API 服务，支持服务的在线浏览申请，为支撑上层应用提供统一支撑。
	拉通应用资源、服务资源、数据资源、知识资源，融合 AI 能力实现服务闭环高阶管理
	提供总集成一体化管理能力，支持多种接入协议，实现应用快速接入
	支持跨多个应用对微服务进行路由规则配置，暴露统一的域名访问方式；
	支持通过对请求的 QPS、线程数进行阈值设置，对 API 进行流量控制

指标项	指标要求
	支持依据 RT、异常比例、异常数对请求进行降级控制
	支持根据 IP 与域名进行黑白名单控制
	支持查看一次请求的完整的调用链路,帮助开发者快速分析和诊断分布式应用架构下的性能瓶颈,提高微服务时代下的开发诊断效率;
	支持开发者将开发的应用或服务申请注册到服务开放系统
	支持开发者在线申请应用或服务
	提供软件著作权证明材料。
系统对接整合	支持广泛的数据源适配、高性能的数据采集和灵活的调度模式,满足各种数据同步需求
	支持设置来源表字段与目标表字段映射方式,以实现不通数据表结构间的数据同步功能,字段映射支持前后缀快速自动匹配模式
	支持常见数据过滤类型包括:空值过滤、枚举值过滤、前后缀匹配过滤、正则过滤等
	支持常见数据清洗类型包括:空值校验与非空校验、前缀校验与后缀校验、数据长度校验、枚举值校验、正则校验等
	支持常见数据转换类型包括:列名转换、行列转换、数据拆分、数据合并、日期格式转换、字符串替换、空值替换、字典值替换、正则转换等
	支持常见数据加/解密算法包括: SM3, SM4, MD5, SHA_1, AES 等
	支持常见数据脱敏规则包括:身份证号脱敏、手机号脱敏、姓名脱敏等
	支持集中的任务中心,任务中心收集各个业务系统的待办任务,通过门户系统来展现,任务中心自动调用消息中心的接口,给业务人员发送任务提醒消息;
	支持任务的弹窗、客户端、首页数量等多种提醒方式
	支持采用集中管理方式实现用户可信身份认证统一管理;
	支持对用户登录时的会话、支持与单点登录模块结合组成跨域的单点登录:
成熟度	▲应用支撑系统支持云化部署,具有自主知识产权的软件著作权证书(须包含关键字:“云支撑平台”)

七、安全产品技术指标

下述技术参数要求中加“▲”标志的为重要响应指标,其余的为一般响应指标。

1、防火墙

技术项	技术要求
基本要求	多核非对称多处理架构，网络层吞吐量 $\geq 6\text{Gbps}$ ，并发连接 ≥ 180 万，每秒新建连接数 ≥ 8 万， ≥ 6 个10/100/1000M自适应电口， ≥ 4 个SFP接口1个Console口，含应用控制、URL过滤、病毒防护、入侵防御功能，及三年应用识别库、URL分类库、病毒特征库、入侵防御特征库升级，3年硬件质保和升有
基础组网	支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式。
	支持VTEP (VxLan Tunnel EndPoint) 模式接入VXLAN网络，并可作为VXLAN二层、三层网关实现VXLAN网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定VLAN、VNI (VXLAN Network Identifier)、远程VTEP，手动管理VXLAN网络；支持MAC、VNI、VTEP静态绑定。
	支持MPLS流量透传；支持针对MPLS流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL过滤、基于终端状态访问控制等安全防护功能，
	支持MTU $\geq 9000\text{byte}$ 的巨型帧Jumbo Frame。
	支持全面的NAT转换配置，包括一对一，一对多，多对一的源、目的地址转换，并至少支持FULL_CONE模式和SYMMETRIC模式。
	支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计
访问控制	支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。
	支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类。
攻击防护	支持基于不同安全区域防御DNS Flood、HTTP Flood攻击，并支持警告、阻断、首包丢弃、TC反弹技术、NS重定向、自动重定向、手工确认等多种防护措施
	能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀
	支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作，可批量设置针对某一分类或全部攻击签名的执行动作
	支持间谍软件防护功能，同时将间谍软件特征库分类，至少包括木马后门、病毒蠕虫、僵尸网络等三种分类；间谍软件防护支持日志、阻断、放行、重置等执行动作，可批量设置针对某一分类或全部攻击签名的执行动作

安全管理	支持基于主机或威胁情报视图，统计网络中存在安全风险的主机数量以及对应的风险等级，至少可查看遭遇风险的时间、威胁类别、情报来源、威胁简介、失陷主机 IP、用户名、资产等信息。
	可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项。
	支持针对“应急响应消息”的手动或自动处置，处置方法至少包括基于漏洞的处置和基于威胁情报的处置
资质要求	《计算机信息系统安全专用产品销售许可证》 增强级

2、主机安全加固

指标项	技术要求
基本要求	采用 B/S 架构设计，管理控制中心高度集成化，无需额外安装或外接数据库即可实现日志存储和分析展示，无需额外安装或对接升级服务器即可实现文件、特征库的升级和分发，支持的 WINDOWS、LINUX 类操作系统，提供 50 个虚拟机授权，集主机防病毒、防火墙、主机入侵防御、Hypervieor 层防护、主机加固、webshell 检测于一体，三年质保和升级服务
	提供已加固的操作系统作为管理控制中心寄宿环境，保证管理控制中心自身安全；
	应支持对已防护的主机统计在线率，对虚拟机是否安装客户端统计整体部署率
	应至少支持 VMware、Citrix、Microsoft、Huawei、H3C、浪潮等国内外主流虚拟化厂商平台，并能够采用一个管理控制中心进行统一管理
主机安全加固	支持双向状态防火墙，提供对出入主机流量进行访问控制与隔离；防火墙支持从 IP、端口、方向、协议、优先级方面进行策略控制；支持防火墙策略的批量复制、删除、修改、停用等操作
	产品应支持入侵防御，可对来自网络层的拒绝服务、缓冲区溢出、木马后门、web 攻击、恶意网络扫描、恶意入侵提权等各类威胁流量的检测与防护。入侵防御规则应不少于 11000 条，并支持按照攻击类型进行分组分类，支持对每一类攻击类型单独开启或关闭防护
	入侵防御支持阻断和检测两种模式
	针对近期爆发流行的永恒之蓝攻击，能够进行有效防护
	支持对主机安全缺陷、配置进行扫描评估，通过打分形式展现不合规和风险程度。能够对 window 操作系统上的策略、服务、组件等进行扫描评估，对 linux 操作系统上的账号、服务、安全参数、进程、配置等进行扫描评估，并给出修复建议，修复建议包括自动修复和手动提示修复
支持对主机的安全加固，针对利用虚拟化漏洞的恶意软件、程序进行拦截并阻止其在主机上运行，提供软件、程序的黑白名单，以减少对系统程序	

	的误拦截风险
	内置 webserv 扫描引擎，针对网站系统恶意 webserv、后门等文件进行扫描防护；能够针对 webserv 文件设定白名单，对文件进行加白处理，避免对核心网站系统文件造成影响

3、防病毒

指标项	技术要求
防病毒	应支持提供快速扫描、全盘扫描、自定义扫描等多种扫描防护模式，支持自定义路径、指定引擎、自定义处理动作的个性化扫描防护。
	提供不少于 3 种病毒查杀引擎，可根据不同虚拟化环境和查杀要求灵活开启与关闭
	支持文件系统实时防护，并可根据系统资源情况设置高、中、低三档不同的防护级别，和选择监控文件的类型。
	应支持对不同压缩包类型文件的监控防护，压缩包监控防护层级可在 1~10 层之间灵活选择，压缩包格式支持不少于 30 种，支持略过特定大小和特定层数的压缩包文件，并可以自定义添加或删除压缩包格式类型
	应支持对病毒文件进行手动加白置黑操作，对目录、文件、扩展名进行信任操作，以提升查杀效率和降低误杀率
	应支持对病毒扫描查杀进行资源占用限制和任务并发控制，防止引发扫描风暴。

4、数据库审计

指标项	指标要求
产品规格	2U 机架式设备，双电源，板载 6GE（含 1 个管理口，1 个 HA 口），1×扩展槽位（可扩展 4GE/4SFP/2SFP+）。2T 存储空间，支持 RAID0/1/5。
性能要求	每秒入库量 6000 条/秒，峰值 SQL 吞吐量 8000 条/秒，并发会话 4500 个，在线日志量 10 亿条语句，归档日志量 40 亿条语句
部署方式	旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计（不需要提供 DBA 账号和任何数据库账户，不需要创建任何数据库账户）。
	支持在目标数据库服务器主机上安装 agent 解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计（不需要提供 DBA 账号和任何数据库账户，不需要创建任何数据库账户），审计平台可以实时监控 agent CPU 使用率、内存使用率、传输包个数。
	agent 参数支持自定义，支持 IP(IPv4\IPv6)、CPU 占用率、内存占用率、本地缓存大小、端口等灵活配置。

	支持审计平台 WEB 界面管理插件，支持插件的配置、唤醒、挂起、中断、升级，审计平台支持远程安装、卸载、下载。
协议支持	支持 Oracle、SQL Server、Db2、Informix、PostgreSQL、Sybase ASE、Sybase IQ、MySQL、MongoDB、SAP HANA、MariaDB、Percona 等主流数据库。
	支持 Hive、HBase、Sentry、Impala、HDFS、ES (Elasticsearch)、GP (Greenplum)、Redis 等大数据平台的审计。
	支持 Teradata、Cache、人大金仓、达梦、神通、南大通用、华为 Guass 等数据库审计。
	支持华为 Guass DB 100、Guass DB 200 数据库。
	支持 SSH 或者 KVM 登录 Oracle、MySQL、SQL Server 数据库服务器后，直接执行的 SQL 操作的审计，不依赖于数据库自身审计功能。
审计功能智能发现	支持跨语句、跨多包的绑定变量名及绑定变量值的审计；支持对超长 SQL 操作语句审计，可以正常记录单条长度小于等于 2M 字节的 SQL 语句内容。
	支持访问来源信息：客户端 IP、端口、数据库名称、数据库用户、OS 用户、访问工具、主机名称、MAC 地址。
	支持应用身份信息：应用客户端 IP、端口、应用用户名、应用 URL 标识、应用 URL 模板、URL、URL 地址参数、URL 消息体参数；支持数据库主机信息：数据库 IP、端口、数据库名、服务名（实例）。
	支持 SQL 语句信息：SQL 标识、操作类型（DDL、DML、DCL 等）、影响行数、响应时间、语句捕获时间、执行结果（DB 应答码、应答错误信息）、受影响对象、SQL 语句、SQL 语句模板、SQL 参数、结果集；支持数据库单向\双向审计。
	支持数据库告警功能，支持对根据 IP、账号、客户端工具名、时间等定制规则进行告警。
	支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址等信息，并且自动添加到审计范围，无需用户提供网段、数据库地址等信息。
结果集审计	支持按照策略进行结果集审计，可以指定敏感表审计结果集。
	支持通过返回行数和内容大小控制返回结果集大小，降低系统开销。
	支持基于结果集的关键字检索。
应用关联	非时间戳的解析方式，采用应用端轻量级插件部署，在并发 1000 个连接的情况下，实现 100%准确关联；以精确方式审计到应用端相关信息，支持应用用户和源 IP 的关联审计；支持 Weblogic、Tomcat、Websphere、Jboss 等主流的应用服务器；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。
安全审计	内置安全特征库规则，如 SQL 注入、缓冲区溢出、权限提升、数据泄露、拒绝服务、访问操作系统、改密码、Bypass FGAC、修改 FGAC、审计、游标注入、访问敏感组件、创建外部 JOB、恶意代码、非系统用户执行命令等常规漏洞。
	应具备漏洞攻击规则库，漏洞攻击规则应至少包括：漏洞名称、CVE 标识、CNNVD、漏洞类型、影响范围等内容。
	支持识别口令猜解攻击，以及在同一个会话里，相同 IP、数据库用户的频次攻击告警。
审计策略	可自定义审计策略。审计策略至少支持 20 个条件，规则各条件之间支持与或非逻辑关系。

	结果集审计支持全局开启，也支持按照具体策略进行结果集审计开启的功能。
	告警数量需支持最大告警数量限制，超过告警阈值之后便不告警。
审计查询	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、数据库服务（实例）名、报文关键字等多种丰富的查询检索条件；支持应用层关联审计查询和关联分析。
	支持不同审计账户，各自查看不同的数据库审计内容，要求：A 账户不能看到 B 账户的数据库审计记录，B 账户不能看到 A 账户的数据库审计记录，安全管理员可以看到所有的审计记录；
	支持将常用的查询条件保存成固定查询模板，方便后续快速查询。
	支持对查询结果中可能存在的敏感数据进行掩码处理，防止敏感数据泄露。
	支持对查询结果以 CSV 文件格式导出到本地。
	在同一套审计系统内可创建子账号，并对不同的子账号授予不同的数据库审计记录的查询检索权限，确保子账号之间彼此数据不可见，避免数据交叉泄露。
	支持 SQL 语句自定义业务化语言翻译。
统计报表	系统提供不少于 40 个报表模型，分别基于全库、数据库组和单库维度进行展现。
	支持合规性报表，如 PCI、等级保护、SOX 法案等专项报表展现。
	支持专项报表展现，针对风险、性能、访问源、账户等信息做专项报表展现。
	支持图表结合展现，支持柱形图、饼状图、条形图，双轴折线图等多种统计图展现形式，基于总体概况、性能、会话、语句、风险多层面展现报表。
	支持按日、周、月等时间周期生成报表。
	支持报表数据后台定期预生成，保障报表数据展现速度。
	支持将报表按指定的时间推送至指定管理员的邮箱。
会话分析	报表支持以 Word、PDF、HTML 等格保存到本地。
	支持会话级检索和详情展现：包括在线的并发会话、活跃会话、失败登录会话等提供专项的分析界面。
	支持失败登录会话查询和统计：包括客户 IP、数据库用户、操作系统用户、工具或应用、数据库应答码、失败原因和失败次数等信息。
对象统计	访问源分析：可展现不同数据库节点的访问源统计、分析状态。
	以操作类型为维度，统计表级别对象被访问次数，可生成行为轨迹图；并可通过对象的访问次数，下钻追溯到该表对象下所有的访问语句详情，以及该表对象访问来源。
统计信息环比	获取同一数据库不同时间段及不同数据库同一时间段的 SQL 语句量和会话量的对比统计数据以及变化趋势。
行为建模	可基于单个数据库建立学习期，默认学习期内行为可信，学习期结束后，产生的数据标记为新型对象、新型语句模板。
数据管理	日志备份与恢复管理，支持审计日志数据的备份与恢复，支持自动备份，备份数据可以选择高性能或高压缩比，支持的备份服务器类型至少包含 FTP、SFTP、NFS 方式，备份记录可以查询。
	支持 KAFKA、SYSLOG 方式进行审计数据外送；KAFKA 外送审计数据内容包括：客户端 IP、客户端端口、客户端 MAC、数据库用户名、数据库实例名等会话信息，SQL 语句参数、SQL 捕获时间、结果集、语句模板、SQL 语句等语句详细信息。

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 IP 地址、数据库用户、时间、对象、应用用户分组，并且分组对象可以直接在规则中引用。
运维管理	审计设备 WEB 界面提供自动诊断功能，可以自动收集实例级参数、策略中心参数、操作系统参数、应用中间件参数。
告警管理	系统告警内容支持网卡异常、分区超限、异常关机、CPU 超限、内存超限、会话超限、包数超限、SQL 数超限、agent 异常等。
	风险告警内容支持触发规则风险内容，并支持根据风险等级高、中、低进行告警通知。
	告警方式包括：邮件、短信、SYSLOG、SNMP、企业微信、审计系统前台界面；支持短信平台对接，发起告警操作。
系统管理	支持三权分立，系统默认设定系统管理员、规则配置员、审计查看员、操作日志查看员等角色，并且可以新建不同用户，分配不同数据库权限和不同的菜单管理权限。
	系统支持 LDAP/AD 域对接，支持 AD 域用户关联审计系统用户，通过 AD 域账户统一登录审计系统。
	具有自身安全审计功能，可以对审计系统的所有用户操作进行审计记录。
产品资质(需提供相关证明文件)	具备公安部颁发的《计算机信息系统安全专用产品销售许可证》，数据库安全审计国标-增强级。
	产品支持 IPv6，具有 IPv6 Ready Logo 认证。
	具备国家保密局涉密信息系统安全保密测评中心颁发的针对信息系统安全监控和审计的《涉密信息系统产品检测证书》。
	产品具备中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》。
第三方评价	▲所投产品的生产厂商在 Gartner 技术成熟度曲线报告的 DAP（数据库审与保护）领域中属于被推荐厂商，提供证明材料。

5、数据库防火墙

指标项	技术规格要求
硬件规格	2U 机架式设备，冗余电源，2GE 管理口，4GE 业务口（2 组 Bypass），配置独立的管理接口，硬盘 2TB。
性能	SQL 峰值吞吐量 6000 条/秒，在线会话 1800 个
数据库类型	支持国际主流数据库类型：Oracle（含 Oracle 18C）、SQL Server（含 SQL Server 2018）、MySQL、DB2、PostgreSQL、SAP HANA、Sybase ASE、Informix 等；
	支持 Hive、HBase 等大数据平台组件。
	支持 Teradata、CacheDB、人大金仓、达梦、神通、南大通用等数据库。
	支持华为 Guass DB 100、Guass DB 200 数据库。

控制模式	无需数据库 DBA 权限，且无需在数据库上安装任何插件，即可对数据库安全进行防护控制。
	支持两种防护模式： 会话阻断：支持依照策略配置对存在风险的会话进行阻断； 拦截语句：支持依照策略配置对会话中的风险语句进行拦截，但不影响会话原有的连接状态。
防护对象	支持通过数据库名称、数据库实例、Schema、表名、字段名、函数等关联信息解析和设置防护规则。
	针对 Oracle 数据库可以区分 PDB/CDB 实例进行防护；
风险识别能力	支持基于 SQL 语法解析实现 SQL 操作的风险识别能力，非正则方式模糊匹配。
	系统具有语句模板抽象能力，能够将语句结构相同但参数不同的语句，抽象为语句模板，并能够根据语句模板配置语句的黑白名单规则，进行拦截和阻断。
	支持按风险语句模板统计具体某一种风险模板语句产生次数、最后执行时间、以及所命中规则。
安全管控	支持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，防止大批量数据泄露。
	支持拦截超过指定行数阈值的批量数据修改、删除操作；支持拦截 no where 引起的整表更新、整表清空的误操作。
	支持拦截指定对象的 ALTER TABLE、ALTER TABLESPACE、DROP DATABASE、DROP TABLE、DROP TABLESPACE、DROP USER、TRUNCATE 等高危操作行为，支持数据库权限变更行为管控。
	支持通过客户端 IP、DB 用户、客户端工具、客户端 MAC、OS 用户、主机名、时间等信息定义非法导出规则，防止非法导出备份。
	支持批量添加敏感对象表，与操作行为进行关联，防止敏感信息泄露和非常规操作。
	支持返回错误码。
	支持口令攻击防护，可基于频次判断失败登录风险。
	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。
	支持结果集内容作为规则判定的条件，结果集包含敏感数据，则直接拦截或阻断。
	结果集作为条件控制支持按全局开启，也可以按照具体规则进行开启。
支持按照策略进行结果集防护，能够采用正则方式对结果集中的内容进行检测，并采取相应的控制动作。	
应用关联防护	非时间戳的解析方式，采用应用端轻量级插件部署，在并发 1000 个连接的情况下，实现 100%准确关联；以精确方式解析到应用端相关信息，支持应用用户和源 IP 的关联防护；支持 Weblogic、Tomcat、Websphere、Jboss 等主流的应用服务器；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。
攻击防护	提供针对利用已公开的数据库漏洞攻击行为进行拦截的虚拟补丁功能；漏洞分类应涵盖：缓冲区溢出、权限提升、拒绝服务攻击等，至少提供 400 个以上虚拟补丁。

	系统提供漏洞补丁规则支持：漏洞名称、CVE 标识、CNNVD 标识、漏洞类型和影响范围。
	支持 SQL 注入、XSS 攻击等外部行为防护。
检索分析	支持风险统计：统计全局和单库的风险命中情况；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。
	支持风险、语句、会话等多维度的详情检索能力。
告警管理	系统告警内容支持网卡异常、分区超限、异常关机、CPU 超限、内存超限、会话超限、包数超限、SQL 数超限等；
	风险告警内容支持触发规则风险内容，并支持根据风险等级高、中、低进行告警通知；
	对满足一定风险级别的访问行为记录到告警日志中，提供给用户进行实时监控和查询；支持风险登录、风险操作、SQL 注入、漏洞攻击检测、口令攻击、频次攻击等风险告警；
	根据按固定周期内设置告警次数，超过告警阈值之后便不告警。
	告警方式包括：邮件、短信、SYSLOG、SNMP、企业微信、审计系统前台界面；支持短信平台对接，发起告警操作；
学习建模	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。通过学习期捕获全量的 SQL 语法，归类形成 SQL 语句模板，可建立信任语句规则对合法的 SQL 模板默认放行策略。
	学习期结束之后自动进入保护期，根据学习期自动建立防护规则，并根据学期建模，构建黑白名单。
	可提供学习期分析报告，对学习期触发的违规行为类型和数量进行统计和分析。
部署模式	支持网桥模式、代理模式、透明代理模式、旁路模式部署；安装部署不需要提供 DBA 账号，在数据库上不需要安装任何软件。
高可用机制	支持 HA 双机主备自动切换，支持策略同步、会话同步机制，保障主备间的一致性。
	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。
支持敏感数据掩码	针对 SQL 语句中的敏感信息，可自定义规则进行数据掩码展现，防止数据二次泄密。
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 IP 地址、数据库用户、时间、对象、应用用户分组，并且分组对象可以直接在规则中引用。
统计报表	支持图表结合展现，支持柱形图、饼状图、条形图，双轴折线图等多种统计图展现形式。
	支持专项报表展现，针对风险、性能、访问源、账户等信息做专项报表展现。
	支持按日、周、月等时间周期生成综合报表；支持风险登陆、高危风险、客户端风险等多种类型报表展现。
	支持报表数据后台定期预生成，保障报表数据展现速度。
	支持将报表按指定的时间推送至指定管理员的邮箱。

	报表支持以 Word、PDF、HTML 等格式保存到本地。
系统管理	支持三权分立，系统默认设定系统管理员、规则配置员、审计查看员、操作日志查看员等角色；可以新建不同用户，分配不同数据库权限和不同的菜单管理权限。
	系统支持 LDAP/AD 域对接，支持 AD 域用户关联审计系统用户，通过 AD 域账户统一登录审计系统。
	具有自身安全审计功能，可以对审计系统的所有用户操作进行审计记录。
数据管理	日志备份与恢复管理，支持审计日志数据的备份与恢复，支持自动备份，备份数据可以选择高性能或高压缩比，支持的备份服务器类型至少包含 FTP、SFTP、NFS 方式，备份记录可以查询。
	支持 SYSLOG 方式进行数据外送。
产品资质	所投产品具备公安部颁发的销售许可证。
	具备国家保密局涉密信息系统安全保密测评中心颁发的针对信息系统安全监控和审计的《涉密信息系统产品检测证书》。
	具备国家信息安全漏洞库兼容性资质证书。
数据库漏洞挖掘能力	▲所投产品的生产厂商具备挖掘国际品牌数据库漏洞能力，所挖漏洞被 CVE 组织收录且具有编号；所投产品的生产厂商具备挖掘国产品牌数据库漏洞能力，所挖漏洞被 CNNVD 或 CNVD 承认且具有编号，至少提供 2 项证明材料。

6、网页防篡改

指标项	指标要求	
资质	通过公安部信息安全产品检测中心检测并获得销售许可证书（增强级） 通过中国信息安全测评认证中心检测并获得中国国家信息安全产品认证证书（3C）；提供证书复印件并加盖公章； IPV6 Ready Logo 认证；提供证书复印件并加盖公章；	
环境支持	操作系统	Windows 2000-2016 32/64 位；Redhat、CentOS、SUSE、Ubuntu 32/64 位
	Web 服务器	Apache 2.0-2.4、IIS6、IIS7、IIS8、IIS10、Java 系列(JBoss、Tomcat、Weblogic、Websphere)等
	数据库	MSSQL、Oracle、Sybase、Informix、DB2、MySQL 等关系型数据库；Mongodb、Cassandra 等非关系型数据库。
	管理方式	B/S 管理方式，Linux 平台部署中心，Windows 中心部署
	核心技术	采用内核文件驱动、Web 核心内嵌双重机制结合 基于特征码、模糊 Hash、脚本虚拟机动态检测 Webshell
	基本功能	网站服务器防篡改、网站服务器防攻击
策略模板	策略模板	可以自定义防篡改&防攻击模板，策略绑定资产实现防护策略批量下发
防篡改功能	文件保护	支持各类网页文件的保护，包括静态和动态网页以及各类文件

		信息
	目录保护	支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码
	一键启停文件保护	一键启停所有对监控端的保护
	篡改规则	支持基于目录、进程、IP、用户等进行设置篡改规则
	自我保护	防篡改程序有自我保护机制
防攻击功能	防病毒	支持多种压缩包、自解压包、符合文档、媒体文件、加密脚本、电子邮件、邮箱文件、可提取文档中嵌入的其它资源的病毒查杀。
	网站漏洞防护	实时防护网站常见的 SQL 注入攻击、XSS 跨站攻击、Web 容器及应用漏洞攻击
		支持文件名解析漏洞防护、禁止浏览畸形文件、敏感信息防泄漏
	CC 攻击防护	智能检测并防御 CC 攻击，保证网站正常服务能力。低中高三级防护：策略验证、Cookie、JS 脚本混合验证、抗图片识别工具的干扰色图片验证
	网站木马	基于特征码、模糊 Hash、脚本虚拟机动态检测 Webshell。
	告警方式	支持邮件，Syslog，短信，SNMPTrap，平台告警多种告警方式

7、Web 应用防火墙

指标体系	指标项	
硬件规格	产品应使用高性能硬件架构，在保证 Web 应用检测的高灵活性的基础上，实现高处理性能。	
	性能要求	设备网络层吞吐率 $\geq 3G$
		设备应用层吞吐率 $\geq 850M$
		设备最大 HTTP 并发连接数 ≥ 200 万
		设备每秒新建 HTTP 连接数 ≥ 5500
硬件接口要求	提供 1 个 10/100M 管理接口、1 个 10/100/1000M HA 口，4 个业务口，支持一个扩展插槽。	
功能要求	应支持智能部署，上线 WAF 设备能够自动感知 Web 网站 IP 和端口。	
	支持安装向导式部署，按照该部署方式可直接部署完成。	
	应具蜜罐检测功能，诱使攻击方对它实施攻击，从而可以对攻击行为进行捕获和阻断。	
	应具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截。	
	具备网站锁功能，对网站进行锁定，可按日期、周期进行锁定时间设置。	

	具备 API 防护功能。
	具备网站一键关停功能)。
	具备源访问区域控制功能，可按照国家、省进行地址访问限制，防止区域性攻击对 Web 网站造成影响。
	应具备客户端访问控制功能，预防恶意客户端进行访问频率的多层次恶意访问。
	应支持获取 Web 安全事件的原始攻击信息。
	Web 安全事件日志存储，应支持主流的服务器操作系统及主流的数据库类型。
	具备多设备拓扑显示功能，可以在界面上以图形化的方式显示当前的部署拓扑。
	支持主主模式且主主模式配置、运行状态进行同步；支持自动执行产品升级，不需要用户每次手动升级特征库。

8、堡垒机

指标项	技术参数要求
硬件形态及性能	准 1U 硬件，含 2*GE 电管理口，4*GE 电业务口，硬盘:1T，硬盘不可扩展；1*RJ45 串口，单电源。最大资产数 100 个，最大字符连接 100 个，最大图型连接 20 个
功能指标	产品内置 VPN 模块，无需与其他 VPN 设备联动，实现运维入口安全接入
	可以通过 socks5/http/ssh 等代理协议连接管理异地云资源区中私有网络的云主机。
	支持自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系，甚至可自动完成授权
	支持在 mac 电脑里使用 navicat 工具通过堡垒机登录 mysql、oracle 等数据库服务器
	需提供用户、资产、授权的增删改查等 API 接口，允许第三方平台调用堡垒机的 API 接口，实现用户、资产、权限自动同步到堡垒机，简化堡垒机配置工作量。
	支持使用本地的 SecurCRT/Xshell/OpenSSH 工具通过 SSH 网关代理方式直接登录字符设备。
	支持 HA+集群部署模式，中心采用 HA，节点可以横向扩展，实现统一登录入口、统一配置同步、审计日志集中查询、实时会话集中监控，以满足业务增长需求。

9、漏洞扫描

技术指标	指标要求
硬件规格	标准 1U 硬件平台，1*RJ45 串口，6*GE 电口，2*USB 口，单电源。 硬盘：1T 内存：16G，可扫描总数量不多于 128 个无限制范围 IP 地址。

功能要求	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。
	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。
	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。
	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。
	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。
	厂商漏洞策略库大于 40000 条；提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与国际 CVE、国内 CNNVD 漏洞库标准兼容。
	系统内置不同的策略模板如针对 Linux、Windows 操作系统等模板，同时允许用户定制扫描策略模板。
	提供采用 SMB、SSH、Telnet、SNMP 等协议对 Windows、Linux 系统进行登录授权扫描。
	具备弱口令扫描功能，提供多种弱口令扫描协议，包括 SMB、RDP、SSH、TELNET、FTP、SMTP、IMAP、POP3、MySQL、MSSQL、REDIS、RTSP 等协议进行弱口令扫描，允许用户自定义用户、密码字典。
	支持发现非默认端口启动的服务，支持服务的协议识别、版本。
	同 IP 不同端口同漏洞的结果应明确给予端口标识。
	支持对误报的漏洞进行修正，避免将误报结果导出。
	支持 7 种以上端口探测方式，如： TCP ACK、TCP SYN、TCP Connect、TCP Null、TCP Xmas、TCP Window、TCP Fin 等。
	支持 HTML、WORD、PDF、XLS 报告格式
配置核查模块	产品提供系统安全配置核查功能，能够对主流操作系统、中间件、无线设备、虚拟设备的安全配置项目进行检查。
	Windows 系统支持提供离线检查工具，将检查结果导入平台查看
Web扫描模块	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 能够检测 GET、POST、User-Agent、Cookie 等多种方式提交的 HTTP 请求参数，并进

	<p>行相应检测；。</p> <p>能够通过 Cookie 的方式支持对带验证码的应用系统进行扫描；</p> <p>存在误报漏洞可通过产品在扫描结果处支持以即时通讯的方式第一时间反馈给厂商协助修改；</p> <p>支持识别国内外主流 Web 应用防火墙品牌；</p> <p>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；</p>
数据库模块	支持 Oracle、Mysql、SQLServer、DB2、informix、达梦、人大金仓的授权数据库漏洞扫描；
产品资质及实力	产品具备《计算机软件著作权登记证》。提供有效证书的复印件
	产品具备公安部的《计算机信息系统安全专用产品销售许可证》（增强级）。提供有效证书的复印件
	产品具备网络关键设备和网络安全专用产品安全认证证书（增强级）。提供有效证书的复印件

10、日志审计

技术指标	技术要求
资质要求	产品获得中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》，需符合 GB/T 20945-2013 《信息安全技术 信息系统安全审计产品安全技术要求 和测试评价方法》（增强级），并提供完整的检测报告复印件；
硬件规格	1 管理口+1HA 口+4 审计口，1 个 Console 口；内存：8GB，磁盘：1T*1；单电源；
处理性能	支持审计 50 个日志源；峰值处理能力（每秒日志解析能力 EPS）：4000 EPS。
日志收集	<p>支持 Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP 协议日志收集；</p> <p>支持使用代理 (Agent) 方式提取日志并收集；</p> <p>支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等；设备厂家包括但不限于：Cisco(思科)、Juniper、联想网御/网御神州、F5、华为、H3C、微软、绿盟、飞塔(Fortinet)、Foundry、天融信、启明星辰、天网、趋势、东软、Nokia、CheckPoint、Hillstone(山石)、安恒信息、珠海伟思、BEA、中国电信、安氏、帕拉迪、APC、Arbor、Clam、戴尔 (Dell)、Digium、东方电</p>

	子、EMC、中国电力科学研究院、Eudora、Google、冠群金辰、Linksys、McAfee、Netapp、NAS(美国国家安全局)、永达、Sonicwall、Vigor、天存、西岭、Symantec(赛门铁克)、Hardened-PHP、Foundertech(方正)、三零盛安、Allot、蓝盾、IBM、金诺网安、网威、Nortel(北电)、Citrix(思杰)、Watchguard、中兴、阿帕奇、Windows 系统日志、Linux/UNIX syslog、IIS、Apache 等； 支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等。
日志分析	以基于日志等级进行过滤 具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件； 内置非法访问、可疑入侵、病毒爆发、设备异常、弱点针对等 5 大类 50 子类的安全分析场景； 三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。
日志查询	支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询； 支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。
综合查询及报表管理	内置合规性报表 1000+种； 内置 SOX、ISO27001、WEB 安全等解决方案包； 内置完善的等级保护合规报表；
用户管理	用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户；
资产管理	资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，扑可以显示资产采集的事件数量被采集资产的状态等信息

11、安全管理中心

指标项	功能参数
硬件规格	标准 2U 上架设备，≥1 个 RJ-45 Console 口，1 个 10/100/1000 Base-Tx 带外管理口，5 个 10/100/1000 Base-T 接口，2 个 USB 口，冗余电源，存储空间：3T 硬盘，16G 内存，提供三年软件升级和原厂质保服务。
性能要求	实际网络环境处理能力（混合包、混合流）：≥1G；最大并发连接数：≥200 万，每秒新建连接数：≥4 万。
攻击检测能力	系统需具备全面的攻击检测能力，可检测常见的 Web 攻击、缓冲溢出攻击、安全漏洞攻击、安全扫描攻击、拒绝服务攻击、木马后门攻击、蠕虫病毒攻击、穷举探测攻击、CGI 攻击等； 系统需具备全面的 Web 应用类攻击检测能力，能够检测各种 SQL 注入攻击、XSS 跨站攻击、Webshell 上传、命令注入、目录遍历、命令执行等攻击行为；

	系统提供的攻击特征不少于 6500 条有效最新攻击规则；
	系统需具备对 Web 类攻击行为双向数据提取的功能，能够详细展示攻击者的请求和返回数据，可以帮助分析者快速研判攻击；
	系统需支持按照协议类型对攻击事件规则的设置检测有效性，协议类型包括 HTTP、DNS、FTP、ICMP、IGMP、IMAP、IP、IRC、MSRPC、NETBIOS-SSN、NNTP、NTALK、PMAP、POP3、RIP、RLOGIN、SMTP、SNMP、SUNRPC、TCP、TDS、TELNET、TFTP、TNS、UDP 等；
	系统需具备攻击检测能力的扩展功能，可提供检测规则自定义的高级接口，接口具备丰富的协议变量，可以自定义配置特协议变量特征值；
	系统需支持 TCP 协议攻击特征自定义，提供 tcp_ack、tcp_fin、tcp_flag、tcp_payload、tcp_syn、tcp_urg、tcp_seq、tcp_rst 等协议变量特征的自定义，支持设置协议变量的操作符，操作符包括等于、不等于、包含、不包含；
	系统需支持 HTTP 协议攻击特征自定义，提供 http_host、http_method、http_passwd、http_url、http_user、http_msgbody、http_msgbody_len、http_cookie、http_user_agent 等协议变量特征的自定义，支持设置协议变量的操作符，操作符包括等于、包含或通过正则表达式设置；
	系统需具备对事件的二次检测能力，即对已生成的事件进行二次分析与统计，并根据统计结果进行报警，支持对统计阈值进行设定的图形化用户接口，通过该图形化接口选择需要统计的基础事件并对阈值进行设置；
	系统需具备对常见的拒绝服务攻击（DDOS）的检测能力，针对特定主机的 TCP FLOOD、UDP FLOOD、ICMP FLOOD 攻击行为进行检测，并支持通过控制界面配置攻击的检测时间和阈值条件；
	系统需具备常见应用的弱口令检测能力，并支持自定义选择弱口令检测条件，可选择的条件组合包括口令长度、口令是否包含用户名、口令是否为数字和字母组合、口令是否全为数字或者字母等；
	系统需具备威胁情报碰撞能力，支持独立的威胁情报库，当内网设备受到外网恶意主机攻击时，可实时产生告警；
	系统需具备对恶意文件的检测能力，系统自带恶意样本库可进行静态检测，并具备与高级可持续威胁检测设备联动进行恶意文件的动态检测能力，具备独立的恶意文件检测告警界面；
	系统需具备独立的专业查毒引擎，独立的病毒库；
	系统需具备攻击事件过滤能力，能够针对 IP 地址或 MAC 地址对攻击告警进行过滤，方便分析人员对正常业务造成的告警进行去除；
威胁分析能力	系统需具备提取攻击信息的能力，告警信息应包括攻击的事件名称、事件威胁等级、事件安全类型、事件攻击类型、事件流行程度、攻击的源 ip、攻击的目的 ip、源端口、目的端口、攻击发生的时间、事件 cve 编号等信息；
	系统需具备提取攻击行为特征信息的能力，针对产生的告警事件，可以对攻击行为特征信息进行提取并展示，方便事件分析人员对攻击行为进行分析；
	系统需具备提取攻击原始报文的能力，针对产生的告警事件，可以对攻击行为的特征数据包进行提取，方便事件分析人员对攻击行为进行分析；
	系统需支持统计近 24 小时木马病毒、端口扫描、拒绝服务等攻击的数量，支持统计近 24 小时攻击事件的 TOP5，支持统计近 24 小时高危事件、中危

	事件、低危事件的网络威胁趋势图；
	系统需具备对攻击一键追溯的能力，支持按照攻击者或被攻击者进行事件追溯，可以以攻击者视角或被攻击者视角展现历史事件数据；
流量统计能力	系统需具备全面的流量统计能力，可以支持实时统计当前网络中的总流量、Web 应用流量、数据库应用流量、邮件应用流量、P2P 应用流量，并按照流量趋势图的形式进行可视化展现；
	系统需具备强大的流量分析能力，支持根据历史流量数据，计算出当前时刻历史均值流量大小，并形成历史均值流量曲线，可以与实时流量曲线进行同时呈现并形成对比，方便分析人员掌握网络流量态势；
	系统需具备完善的流量告警能力，支持按照历史流量同期对比和设置流量阈值两种方式配置告警参数，告警级别包含偏低、偏高等多种类型；
资产管理能力	系统需具备自动发现用户网络资产的能力，可自动上报网络中的存活资产，并支持获取内网资产的暴露面信息和资产指纹信息；
	系统需支持自定义业务系统资产分组的能力，可将发现的资产自动划分至所属的业务系统资产分组，业务系统资产分组应至少支持五级；
	系统需具备未知（非法）资产入网发现的能力，可以及时发现违规入网的 IP 地址，防止内网资产乱接乱用；
流数据采集与互联分析能力	系统需具备将网络流量数据解析成资产设备间互联访问关系的能力，能够详细记录源 IP、源 IP 分组、源 IP 地区、目的 IP、目的 IP 分组、目的 IP 地区、目的端口、传输层协议、服务名称、流量大小、频次等数据信息；
	系统需具备自动发现内部资产与互联网设备互联的能力，并能准确显示互联的方向，能够区分是内部服务器向外发起连接还是外部设备向用户内部服务器发起的连接；
	系统需具备将网络流量按照业务系统资产分组可视化展示互联关系的能力，支持拓扑图的形式展示内网和互联网以及内网各域之间互联情况，方便分析人员全面掌握全网访问关系；
	系统需具备可视化展示各业务系统资产分组互联关系的能力，支持查看资产分组内的互联情况和资产分组之间的互联情况，方便分析人员分析；
	系统需具备监控违规访问互联网和非法连接的能力，支持对网络中产生的违规互联进行实时告警，并用红色连线在互联拓扑图中进行标识，方便分析人员快速发现违规外联和非法访问；
	支持内置网络主机异常行为特征算法（非数据包特征），通过主机的互联行为可以主动发现内网具有一定威胁的异常主机，包括中招蠕虫主机、网络扫描主机等；
	系统需具备应用层协议解析能力，支持解析 HTTP 协议 URL 数据、DNS 协议域名数据等应用层数据信息；
系统管理能力	系统需具备检测策略管理能力，支持检测策略规则可以按照协议类型、攻击类型、安全类型、影响系统、影响设备等多个维度进行展示，方便运维人员按照不同的业务场景创建检测策略集；
	系统需具备探针设备的监控能力，实时监控检测引擎的连接状态、当前使用的检测策略集和设备的资源配置信息；
	系统需具备邮件告警能力，支持将发现的攻击告警信息通过邮件的方式发送至指定的

	邮箱地址；
	系统需具备用户管理能力，支持三权分立原则，系统具有用户管理员、审计管理员、配置管理员，支持创建不同的配置管理员，并赋予不同的授权角色，控制管理员的配置权限；
	系统需具备绑定管理员用户 IP 地址的能力，支持对管理员用户的 IP 地址进行绑定，防止非法 IP 的使用账号访问设备；
报表分析能力	系统需具备多种数据报表类型，每种报表类型的数据统计方式应从不同的维度进行分析，方便不同层次的技术人员进行数据汇总；
	系统需具备数据交叉统计能力，支持按照事件名称、源地址、目的地址等多个维度对事件进行交叉统计分析，帮助分析人员快速定位攻击；
	系统报表需支持如下格式：HTML、PDF、EXCEL、WORD，所生成的报表可以自动发送到多个邮箱，能辅助用户查阅；
	系统报表需支持手动立即执行、周期性自动执行两种执行方式；
部署能力	设备需支持多个监听口同时接收业务流量，各监听口对网络数据的分析和攻击检测互不造成影响；
	系统需具备分布式部署能力，可以支持一个管理中心管理多台检测引擎的部署方式，方便攻击告警信息在统一平台展示；
	系统需具备多级部署能力，可以支持管理中心设备级联部署，方便大型多级网络的统一管理和分析；
日志配置	系统需具备攻击日志外发能力，支持通过 syslog 方式将告警日志发送日志服务器或分析平台，也可将告警日志输出至 kafka 服务器；

八、其他技术要求

根据业务办理的要求，系统承载硬件满足所有系统提出的硬件承载需求时，系统性能需满足以下指标：

1.单点登陆

- 用户登录门户系统后，使用各业务系统不需要重新登录；
- 用户登录后，在各业务系统间跳转不需要重新登录。

2.耦合度

- 在不影响性能的基础上，各业务系统尽量松耦合；
- 系统集成后不影响各业务系统的单独使用；
- 整合资源之间不彼此影响耦合度。

3.灵活性

- 系统应具有良好的扩展性和可移植性；

- 采用模块化的设计，便于功能单元配置和部署；
- 系统操作界面可根据用户要求进行配置，体现用户个性化；
- 灵活的权限管理和角色访问策略，采用多级管理，便于三级管理模式的实行；
- 跨平台支持；
- 接口做到独立于应用程序，确保在应用更换和升级的情况下不需要重新设计接口；
- 应用层和数据库应分离开。

4.便捷性

- 系统设计过程需考虑到易于操作、易于使用、界面友好等问题，无需培训或只需少量的培训即可使用。

5.可靠性

- 要保证核心业务部分能可靠运行，建立故障转移群集、负载均衡群集，保证关键部分非单点工作的开展。

6.稳定性

- 在稳定性上，系统应该可以全年稳定连续运行，故障时间不超过千分之一，导致业务连续停止时间不超过 3 小时。一个月内不需要重启服务器不间断访问系统，系统的运行效率不会明显降低。

7.时间特性

- 简单事务处理（包含各类信息录入、修改、查询业务、主要页面平均响应时间等）≤3s；
- 事务处理查询时间平均不超过 3 秒，普通应用查询时间平均不超过 2 秒，统计分析类查询时间平均不超过 5 秒系统运行时峰值服务 CPU 所占比不超过 60%，内存所占比不超过 80%；
- 7*24 小时不间断运行；

九、实施要求

投标人需提供本项目的实施方案，实施方案至少要包含进度计划、人员配置、安装调试测试、质量保障方案等内容。

实施方案需保障阶段划分合理、保障措施到位，具备可执行性。

十、验收要求

1、系统在各阶段验收前，需通过第三方机构测试；系统在竣工验收前，需通过等级保三级测评。

2、项目阶段性及终期成果完后，乙方应参加甲方组织的评审会并作项目汇报。

3、验收方法：甲方组织的评审会或汇报会评审（评审会或汇报会评委由买方确定），并通过最终评审。

十一、培训要求

投标人应借助自身的资源优势和技术优势为用户方提供优质的培训服务。投标人应选择具有较高技术水平、丰富实际工作和教学经验的技术人员担任教师，并准备有关培训教材，对系统的实际应用人员和技术人员进行培训。

具体培训时间根据甲方实际要求，投标人需提供完整的培训计划，包括培训方式、课程内容、人数、时间、地点。

十二、售后服务要求

1.项目维护期要求

自项目验收通过之日起，成品软硬件产品提供 3 年免费质保，定制开发的软件提供不少于 2 年的免费维护服务。

维护服务内容包括：软件系统维护、功能完善或微调、性能调优、故障检测，保证所开发的软件正常运行。

2.维护期内的服务要求

质保期内，如系统出现问题，供应商必须在接到报故障信息后 15 分钟内响应，2 小时内解决问题。

3.维护期后的服务

投标人向采购人承诺维护期满后，将继续提供维护工作，并明确提出服务的方式、范围和收取费用标准。

十三、知识产权和保密要求

本项目软件开发的相关知识产权为采购人所有，中标须提供定制本项目软件开发的相关知识产权为采购人所有，中标须提供定制件全部源代码及相关技术文档。因第三方软件侵权造成的损失由中标人自行承担。

投标人中标后需同用户签订保密协议，严格遵守保密协议，未经用户允许不得将相关资料、信息泄露给第三方，不得利用此数据进行任何侵害招标方的行为，泄露国家秘密须承担法律责任。

第6章 评标方法和标准

评标委员会将按照本项目招标文件第 1 章及本章的规定进行评标工作，采购代理机构负责评标的组织工作。

一. 评标依据

1. 《中华人民共和国政府采购法》；
2. 《中华人民共和国政府采购法实施条例》；
3. 《政府采购货物和服务招标投标管理办法》（财政部第 87 号令）；
4. 《财政部关于加强政府采购货物和服务项目价格评审管理的通知》；
5. 《评标委员和评标方法暂行规定》；
6. 法律法规的相关规定
7. 本项目招标文件。

二. 评标原则

1. 公平、公正、科学合理评标；
2. 评标委员会由采购人代表和评审专家组成，成员人数为五人以上单数。其中，评审专家不得少于成员总数的三分之二。采购数额在 1000 万元以上、技术复杂的项目，评标委员会成员人数应当为 7 人以上单数。评标委员会由招标采购单位从河南省财政厅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，参加评标的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。

三. 评审顺序

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）规定由采购人对投标人的资格性进行审查。

评审因素		评审标准
资格性 审查	有效期的营业执照	提供扫描件
	法定代表人身份证明书、法定代表人授权委托书（附法人身份证明扫描件及授权代表身份	提供授权书及身份证扫描件
	投标保证承诺书	按招标文件要求提供承诺书
	财务状况报告	2018 或 2019 年度的财务审计报告，财务审计报告应具有 2 名及以上注册会计师盖章和签字。成立时间不足 1 年的，提供银行出具的资信证明或财政部门认可的政府采购专业担保机构出具的投标担保函
	纳税和社保	2019 年 6 月 1 日以来任意 3 个月纳税证明材料和社会保障资金缴纳相关材料
	具有履行合同所必需的设备和专业技术能力的书面承诺	提供承诺书
	投标人提供参加政府采购活动前三年内在经营活动中没有重大违法、违纪行为书面声明	提供声明函

	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的声明函	提供声明函
--	--	-------

2. 评标准备工作

- 2.1 核对评审专家身份和采购人代表授权函；
- 2.2 宣布评标纪律，集中保管通讯工具；
- 2.3 公布投标人名单，告知评审专家应当回避的情形；
- 2.4 组织评标委员会推选评标组长；

3. 符合性审查工作

符合性审查是指依据招标文件的规定，从商务和技术角度对投标文件的有效性和完整性进行审查，以确定是否对招标文件的实质性要求做出响应，填写“符合性审查表”。

评审因素		评审标准
符合性审查	投标人名称	与营业执照、资质证书一致
	投标文件电子签章	按招标文件要求格式电子签章
	报价唯一	只能有一个有效报价
	投标有效期	符合招标文件要求
	不同投标人投标文件制作机器码是否一致	一致，则为无效投标
	其他实质性要求	符合招标文件的其他实质性要求

4. 要求投标人对投标文件有关事项作出澄清或者说明

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。

5. 对投标文件进行比较和评价

5.1 如本项目评标方法为最低评标价法，评标委员会在审查投标文件满足招标文件全部实质性要求后，按投标报价从低到高顺序确定中标候选人。

除了算术修正和落实政府采购政策需进行的价格扣除外，不得对投标人的投标价格进行任何调整。

5.2 如本项目评标方法为综合评分法，评标委员会对满足招标文件全部实质性要求的投标文件，按照招标文件规定的评审因素的量化指标进行评审打分，以评审得分从高到低顺序确定中标候选人。

评标委员会每位成员独立对每个有效投标人的投标文件进行评价、打分；然后汇总每个投标人的得分，计算得分平均值，以平均值由高到低进行排序，按排序顺序推荐中标候选人。分值计算保留小数点后一位，第二位四舍五入。

6. 确定中标候选人名单，或者根据采购人委托直接确定中标供应商。

7. 核对评标结果。

四. 评审标准中须考虑下列因素：

1. 根据《政府采购促进中小企业发展暂行办法》（财库[2011]181号）、《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）和《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，对满足价格扣除条件且在投标文件中提交了《投标人企业类型声明函》、《残疾人福利性单位声明函》或省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件的投标人，其投标报价扣除 6 %后参与评审。对于同时属于小微企业、监狱企业或残疾人福利性单位的，不重复进行投标报价扣除。（详见评标标准）。

2. 联合协议中约定，小型、微型企业和监狱企业的协议合同金额占到联合体协议合同总金额 30%以上的，可给予联合体 2%的价格扣除。（详见评标标准）。

联合体各方均为小型、微型企业和监狱企业的，联合体视同为小型、微型企业和监狱企业

3. 推选中标候选人：

采用综合评标法，则：根据采购需要、商务、技术均能满足招标文件要求，按评标委员会评出的综合得分，由高到低顺序排列，推荐 3 名中标候选人（如最得分相同的，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）。

五、综合评分标准

评委将根据评分标准，分别对通过符合性审查、资格性审查的投标人，进行综合评分。

具体评分标准如下：

序号	评分因素		评分标准	分值
一、	价格部分 (10分)	投标报价	满足招标文件要求且投标报价最低的为评标基准价，其投标报价得 10 分，其他投标人的投标报价得分按照下列公式计算：投标报价得分=（评标基准价/投标报价）×价格权值（10%）×100，四舍五入小数点后保留两位。 （评标委员会在评审时发现投标人的报价明显低于成本价的，应当要求投标人书面说明并提供相关证明材料。投标人不能当场合理说明原因并提供证明材料的，评标委员会应将该投标人的投标文件作无效处理，并在评审报告中说明。）	10
二、	商务部分 (35分)	投标人业绩	投标人自 2018 年 1 月 1 日（以合同签订时间为准）以来具有以下合同业绩：投标人具有“互联网+监管”或政务服务信息化类项目业绩（内容涉及省本级各相关厅局），提供省级及以上证明合同每个得 2 分（合同采购主体须为省厅、局、委、办及以上部门），	6

			<p>最多得 4 分；市县级证明合同每个得 0.5 分(合同采购主体须为市县局、委、办或以上部门)，最多得 2 分。（提供完整采购合同扫描件）</p>	
		综合技术实力	<p>1. 投标人具有厅局级及以上业务系统部署上云和提供云平台服务的能力或经验，提供近三年以来厅局级及以上业务系统部署上云和提供云平台服务的证明材料，每提供一份得 2 分，最多得 6 分。</p> <p>2. 投标人参与过政务服务或政务数据类标准制定，并成功发布实施。提供国家市场监督管理总局/国家质量技术监督局发布的标准规范证明材料，得 4 分；提供省市场监督管理局/省质量技术监督局发布的标准规范证明材料，得 2 分。本项共 6 分。</p> <p>说明：须提供证明材料扫描件加盖投标人电子公章</p>	12
		投标人资质证书	<p>1. 投标人具有 CMMI3 级及以上资质证书的计 2 分，其他不计分；</p> <p>2. 投标人具有 ISO/IEC 20000-1 信息技术服务管理体系认证证书，此项共 2 分；</p> <p>3. 投标人具有 ISO/IEC 27001 信息安全管理体系认证证书，此项共 2 分；</p> <p>4. 投标人具有 CCRC 信息安全服务资质——信息系统软件安全开发服务资质认证证书，得 2 分；</p> <p>5. 投标人具有 ITSS 信息技术服务运行维护标准符合性证书得 1 分；</p> <p>6. 投标人同时具有以下 3 类证书得 2 分，缺项不得分，此项共 2 分：</p> <p>（1）质量管理体系认证证书；</p>	11

			(2) 环境管理体系认证证书; (3) 职业健康安全管理体系认证证书。 说明: 提供相关证书扫描件并加盖投标人电子公章	
		项目团队能力	1. 投标人委派的项目经理同时具有 PMP 认证证书, 系统集成项目管理工程师证书得 1 分, 否则不得分。 2. 本项目开发团队人员数量不少于 20 人, 项目组人员含有信息系统项目管理师、系统架构师、系统分析师、系统规划与管理师、ITIL、软件设计师、注册信息安全专业人员 (CISP) 等证书, 每提供一个证书得 0.5 分, 共 3 分; (说明: 提供人员证书扫描件和 2020 年以来近三个月投标人为其交纳社保的证明材料)	4
		售后服务	1. 根据投标人所提供的售后服务方案, 综合评比后进行打分, 内容合理全面得 1 分, 内容较合理可行 0.5 分, 内容不甚合理且不完整 0 分。 2. 提供售后服务承诺书, 满足招标文件要求得 1 分, 不满足或不提供不得分。	2
三、	技术部分 (55 分)	重要响应指标	1. ▲标注为重要响应指标, 全部满足得14分, 每有一项不满足扣2分, 扣完为止; 2. 其它一般性指标要求, 全部满足得1分。 评分依据: 投标人根据招标文件中《成品软件技术指标》、《硬件产品技术指标》章节要求响应, 提供相关证明材料	15
		项目需求分析	根据招标文件中描述, 对安全智能化监管平台需求分析的合理性、完整性、	3

			<p>可行性等方面进行评价：</p> <p>1. 内容合理，完整全面、切实可行，完全满足招标文件要求的，得 3 分；</p> <p>2. 内容较合理，较完整全面，较可行，较满足招标文件要求的，得 2 分；</p> <p>3. 内容表述不合理、不完整全面，不能满足招标文件要求的，0 分。</p>	
		系统架构设计	<p>根据投标文件中的系统架构设计方案的完整性、科学性、合理性、可行性，及设计框架和设计思路具有先进性和科学性，并能满足项目建设需求等方面进行评价：</p> <p>1. 内容合理，完整全面、切实可行，完全满足招标文件要求的，得 4 分；</p> <p>2. 内容较合理，较完整全面，较可行，较满足招标文件要求的，得 2 分；</p> <p>3. 内容表述不合理、不完整全面、未能全面满足招标文件要求，0 分。</p>	4
		主要功能开发要求	<p>五大业务域应用系统。开发部署监督管理业务域子系统、监测预警业务域子系统、指挥救援业务域子系统、决策支持业务域子系统和政务管理业务域子系统。根据投标人方案进行综合评价，此项共 4 分。</p> <p>1. 内容合理，完整全面、切实可行，完全满足招标文件要求的，得 4 分；</p> <p>2. 内容较合理，较完整全面，较可行，较满足招标文件要求的，得 2 分；</p> <p>3. 内容表述不合理、不完整全面、未能全面满足招标文件要求，0 分。</p>	4
		数据资源管理能力	<p>建设数据资源管理系统。包括信息资源规划、数据整合汇聚、应急管理数据资源池建设、数据治理系统、数据服务系统和数据应用系统。根据投标</p>	3

			人方案进行综合评价，此项共 3 分。 1. 内容合理，完整全面、切实可行，完全满足招标文件要求的，得 3 分； 2. 内容较合理，较完整全面，较可行，较满足招标文件要求的，得 1.5 分； 3. 内容表述不合理、不完整全面、未能全面满足招标文件要求，0 分。	
		政务云服务能力	根据招标文件要求，提供本监管平台系统在省级政务云部署上云方案，根据技术支持和安全保障服务的合理性、全面性及是否满足招标文件要求等方面进行评价，此项共 3 分。 1. 内容合理，完整全面、切实可行，完全满足招标文件要求的，得 3 分； 2. 内容较合理，较完整全面，较可行，较满足招标文件要求的，得 1.5 分； 3. 内容表述不合理、不完整全面、未能全面满足招标文件要求，0 分。	3
		平台及数据对接能力	依据投标人所提供的对接河南省“互联网+监管”、河南省省级政务服务平台以及数据共享交换能力技术方案，进行综合评价，此项共 4 分。 1. 内容合理，完整全面、切实可行，完全满足招标文件要求的，得 4 分； 2. 内容较合理，较完整全面，较可行，较满足招标文件要求的，得 2 分； 3. 内容表述不合理、不完整全面、未能全面满足招标文件要求，0 分。	4
		系统的安全及备份措施	根据系统是否具有可靠的安全机制，能够确保系统和数据的安全性和完整性等方面进行评价。此项共 3 分。 1. 内容合理，完整全面、切实可行，完全满足招标文件要求的，得 3 分； 2. 内容较合理，较完整全面，较可行，	3

			较满足招标文件要求的，得 1.5 分； 3. 内容表述不合理、不完整全面、未能全面满足招标文件要求，0 分。	
		项目实施计划	根据供应商所提供的项目实施计划进行评分，按照项目工期综合考虑相关标准规范制定、开发计划、测试计划、集成计划、验收计划等内容进行打分，此项共 3 分。 1. 内容合理，完整全面、切实可行，完全满足招标文件要求的，得 3 分； 2. 内容较合理，较完整全面，较可行，较满足招标文件要求的，得 1.5 分； 3. 内容表述不合理、不完整全面、未能全面满足招标文件要求，0 分。	3
		培训方案	根据投标文件中培训实施计划，对培训方案完整性、合理性、切实可行性进行评价。此项共 3 分。 1. 内容合理，完整全面、切实可行，完全满足招标文件要求的，得 3 分； 2. 内容较合理，较完整全面，较可行，较满足招标文件要求的，得 1.5 分； 3. 内容表述不合理、不完整全面、未能全面满足招标文件要求，0 分。	3
		系统演示	为保证应用系统满足采购人需求，投标人应提供时长 15 分钟以内的真实系统演示视频。采用录屏形式演示，以 MPG 格式存 U 盘密封包装提交，注明投标单位和项目名称。演示视频于投标截止时间前递交至河南省公共资源交易中心。 一、一企一档一码 【本项演示 3 分，每演示一项得 1 分，不演示不得分】 1、演示企业数据录入过程，实现数据核查检测、自动打分，安全码赋码功	10

			<p>能；</p> <p>2、演示查看企业详情，并能够查看企业整体档案信息。</p> <p>3、演示通过手机微信扫码查看已填报企业档案信息；</p> <p>二、安全生产双重预防体系</p> <p>【本项演示 4 分，每演示一项得 1 分，不演示不得分】</p> <p>1、演示企业风险分级管控全流程功能，展现从风险点划分到形成风险管控清单的过程；</p> <p>2、基于风险管控清单，演示隐患排查、整改、验收全流程功能；</p> <p>3、演示通过手机 APP 进行风险扫码一键排查隐患功能；</p> <p>4、演示风险辨识方法自定义功能。</p> <p>三、应用系统：指挥救援</p> <p>【本项演示 3 分，每演示一项得 1 分，不演示不得分】</p> <p>1、演示应急事件发生时，对周边资源、风险、次生衍生灾害等进行分析；</p> <p>2、演示应急事件发生时，根据数据模型推演当前及未来灾害变化趋势；</p> <p>3、演示应急物资推荐、作战指挥区域推荐、人员疏散推荐、有毒物质扩散、灾损计算等功能。</p>	
--	--	--	--	--

第7章 政府采购合同

河南省安全生产智能化监管平台 项目合同

项目编号：

甲方： 河南省应急管理厅

乙方：

签订时间：

签订地点：

为明确甲乙双方的权利与义务，根据《中华人民共和国合同法》及相关法律法规的规定，本着互惠互利的原则，双方就河南省安全生产智能化监管平台有关事宜达成以下协议以共同遵守：

第一条 项目概况

项目名称：河南省安全生产智能化监管平台

项目地址：

双方委派的工程代表：

甲方代表： ，联系电话：

乙方代表： ，联系电话：

第二条 采购内容

1. 根据招标结果，乙方负责河南省安全生产智能化监管平台项目的建设实施工作。项目依托省政务云、省电子政务外网建设河南省安全生产智能化监管平台，平台主要覆盖省、市、县三级应急管理机构，实现省、市、县三级应用省级统一部署，各市县可根据当地实际需要进行相关功能的补充和完善建设。平台包括一个数据资源管理系统、一个应用支撑系统、五大业务域相关业务应用系统以及安全系统。计算、存储和网络资源均由省政务云支撑满足。具体内容为：

（1）建设五大业务域应用系统。部署监督管理业务域子系统、监测预警业务域子系统、指挥救援业务域子系统、决策支持业务域子系统和政务管理业务域子系统；

（2）建设数据资源管理系统。包括信息资源规划、数据整合汇聚、数据资源池、数据治理、数据服务系统和数据应用系统；

（3）建设应用支撑系统。部署数据治理 ETL 数据抽取工具，部署统一用户、统一认证、统一 workflow 等基础支撑软件，部署移动服务平台软件，部署基于微服务的服务开放系统，进行系统对接整合；

（4）建设安全系统。部署防火墙设备 2 台、主机安全加固设备 2 台、防病毒设备 2 台、数据库审计设备 1 台、数据库防火墙 1 台、网页防篡改设备 1 台、Web 应用防火墙 1 台、堡垒机 2 台、漏洞扫描设备 2 台、日志审计设备 2 台和安全管理中心设备 1 套；

（5）标准规范一套。

（6）完成与河南省“互联网+监管”系统、河南省政务服务网及其他相关系统的

对接服务等。

上述建设内容涉及的需求、设计、软硬件采购、实施、培训、维保及相关服务等全部工作，以及与相关单位沟通协调等所有相关事宜均由乙方负责。

2. 甲方审定乙方制定的本项目工作方案，乙方根据甲方审核确定的工作方案进行项目实施，其间乙方涉及到的与项目实施有关的各项事宜均由乙方自行解决，涉及乙方不能确定的技术问题或特殊突发情况应和甲方协商解决。

3. 项目建设内容详见招标文件要求。

第三条 合同价款与结算

1. 合同总价款为：元，人民币大写：整，包含项目内容所涉及的各项费用及税金。

2. 付款方式

(1) 合同签订后 个工作日内，甲方向乙方支付合同价款的 ，即 元（大写： ）；

(2) 初验合格后，甲方在收到乙方票据并确认无误后 个工作日内向乙方支付合同价款的 ，即 元（大写： 整）；

(3) 终验合格后，甲方在收到乙方票据并确认无误后 个工作日内向乙方支付合同价款的 ，即 元（大写： 整）；

(4) 质保期内质保金为合同额的 5%，按照成品软硬件 3 年质保、定制开发软件系统 2 年质保的期限，每年质保验收合格后支付该年度对应的质保金，为合同价款的 ，即 元（大写： 整）；

(5) 甲方将合同款付至乙方指定帐户；

(6) 乙方在甲方支付合同款项前，应先按各期付款数额向甲方开具符合国家法律法规和标准的税务发票。

第四条 技术资料

1. 乙方应按甲方规定的时间提供项目有关技术资料。

2. 未经甲方事先书面同意，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、软件或资料提供给与履行本合同无关的任何其他人。

3. 未经乙方书面同意，甲方不得将乙方或其关联企业、合作企业等拥有专有知识产权的产品及技术提供、销售、出租、出借、转让或提供许可、通过信息网络传播或其他形式给任何第三方或者应用于本项目外的其他项目。

第五条 知识产权

1. 乙方应保证所提供的全部软件产品、服务均不会侵犯任何第三方的知识产权。

2. 在本项目实施过程中，甲方利用乙方提交的技术服务工作成果所完成的新的定制技术开发成果，归甲乙双方共有。

3. 在本项目实施过程中，乙方利用甲方提供的技术资料和工作条件所完成的新的定制技术开发成果，归甲方所有。

4. 甲方享有本项目实施过程中产生的知识成果及知识产权。

第六条 产权担保

1. 乙方保证对所交付的软件产品均具有合法权益，且其上未设定任何担保措施或被司法查封等产权瑕疵或权利限制。

2. 如因第三方向甲方提出侵权索赔或其他主张的，由乙方承担责任，并赔偿甲方因此受到的经济损失和商誉损失。

第七条 工期

1. 建设工期要求：合同签订后月内完成调测部署、上线运行。

第八条 培训

乙方向甲方提交《培训计划》，在得到认可后组织开展相关培训工作。培训内容包括系统功能说明、系统应用、系统管理、用户操作、常见问题处理等。

第九条 调试和验收

1. 验收标准：以采购文件中各模块功能指标项要求和响应文件的说明为基础，按照国家相关标准要求组织验收。

2. 项目验收前，系统需由具备国家认可的软件测试资质第三方公司测评，功能和性能测试的结果为通过，所需费用全部由乙方承担。系统通过信息安全等保测评后方可进行项目最终验收，所需费用全部由乙方承担。

3. 乙方完成基本建设内容，系统正常运行，达到初验条件，由乙方书面提出初验申请，甲方对本项目进行验收，验收通过后，甲方出具初验报告给乙方。

4. 初验通过且系统稳定运行后，由乙方书面提出终验申请，由甲方对本项目进行验收，验收通过后，出具终验报告。

5. 验收前，乙方应对系统做全面检查和对验收文件进行整理，并列清单，作为甲方验收和使用的技术条件依据，检验的结果应随产品交甲方。

6. 甲方对乙方提供的软件产品在使用前进行测试时，乙方需负责安装并培训甲方及业主方的使用操作人员，并协助甲方一起调试。

7. 验收时乙方在现场，验收完毕后作出验收结果报告，验收费用由乙方负责。

第十条 保密条款

1. 甲乙双方应恪守因签署或履行本合同而获知的对方政府/商业信息及其它政府/商业秘密。任何一方如将获知的对方政府/商业秘密泄露给第三方，应赔偿因泄密而给对方造成的一切损失并承担相应的法律责任。

第十一条 质量保证及售后服务

1. 质量保证期：成品软硬件产品为终验后年，定制开发软件为终验后年。

2. 乙方提供的成品软硬件产品及定制开发系统在质保期内因产品本身的质量问题发生故障，乙方应负责免费更新。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：

(1) 开发更新：由乙方承担所发生的全部费用。

(2) 贬值处理：由甲乙双方协议定价。

(3) 拒收处理：乙方应退还甲方支付的合同款，同时应承担该产品的直接费用（保险、检验、款项利息及银行手续费等）。

3. 在质保期内，乙方应对产品（硬件、软件和服务）出现的质量及安全问题负责处理解决并承担一切费用。

4. 乙方负责质保期系统故障处理服务、缺陷管理、系统漏洞处理、质量管控、技术支持、应用系统升级服务、日常巡检与安全保障服务、应急处理和数据维护等工作，提供7×24小时质保处理响应。

第十二条 违约责任

1. 甲方应按照合同约定按时向乙方支付项目款，每逾期一天，甲方应按合同价值总额的1%标准向乙方支付违约金，违约金总额不超过相应合同价值的3%。

2. 合同签订后确因乙方质量问题造成返工、延误工期、给甲方造成损失的，乙方应支付给甲方违约金。

乙方工期延误：完工期限每逾期一天，乙方向甲方支付金额为合同款的1%的逾期违约金，逾期违约金上限为合同总额的3%；因乙方原因造成工期延误超过60天的，甲方有权解除本合同。

乙方其他违约：乙方不履行合同义务或不按合同约定履行义务的，甲方有权终止合同，并由乙方承担由此带来的一切损失。

3. 本合同生效后，除甲乙双方一致同意或不可抗力外，双方应认真履行。

4. 乙方工作质量达不到合同规定的，甲方有权要求乙方予以完善和改进，由此产生的一切费用由乙方负责。

第十三条 不可抗力事件处理

1. 本合同所指不可抗力系指：地震、风暴、水灾或其他自然灾害、瘟疫、战争、暴乱、敌对行动、公共骚乱、公共敌人的行为、政府或公共机关禁止、国家法律法规变更、政策调整、监管部门的相关规定或指令调整等任何一方无法预见、无法控制和无法避免的情况。

2. 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，则合同履行期可经各方协商后延长，其延长期与不可抗力影响期相同。

3. 不可抗力事件发生后，遭遇不可抗力的一方应在发生不可抗力事件后的 3 日内书面通知对方，并向对方提供发生不可抗力及其持续期的适当证明，并应尽其最大努力终止不可抗力事件或减少其影响，否则，不能免除相应责任。

4. 不可抗力事件延续 120 天以上，甲方、乙方应通过友好协商，确定是否继续履行合同；如因此终止合同的，双方互不承担违约责任。但是因一方迟延履行合同义务后，发生不可抗力的，不可免除责任。

第十四条 争议解决方式

1. 本合同未尽事宜，双方协商解决。经双方协商一致，合同条款可以予以变更或终止。甲乙双方在履行合同过程中发生争议，应友好协商解决，协商不成的，双方一致同意向甲方所在地人民法院提起诉讼。

第十五条 合同变更、终止

1. 本合同生效后，未经双方协商一致，达成书面协议，任何一方不得擅自变更本合同。如果变更本合同条款或就未尽事项签署补充合同，应经双方共同协商达成一致，并签署书面文件。

2. 除双方经协商一致，或依据法律、行政法规之规定，任何一方均无权终止本合同或取消其中某一部分。

第十六条 合同生效及其它

1. 双方按照本合同确定的联系方式向对方送达书面通知文件，自发出时视为履行完毕通知义务，本条通知方式可直接适用于因履行本合同引发的司法程序。

2. 本合同经甲乙双方授权代表签字或盖章并加盖单位公章后生效。一式陆份，双

方各执叁份，具有同等法律效力。

3. 本次的招标文件、乙方的投标文件以及承诺书等均是合同的组成部分，与本合同具有同等法律效力，乙方严格按照相关约定履行合同义务。

甲方（盖章）：

乙方（盖章）：

法定（授权）代表人：

法定（授权）代表人：

地址：

地址：

附件 1：详细报价清单