河南省行政审批和政务信息管理局2026年度局属政务信息系统运维项目

招 标 文 件

采购编号：豫财招标采购-2026-526

采 购 人：河南省行政审批和政务信息管理局

采购代理机构：河南省机电设备招标股份有限公司

二〇二六年五月编制

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。

目 录

第一章 招标公告

河南省行政审批和政务信息管理局2026年度局属政务信息系统运维项目 招标公告

项目概况

河南省行政审批和政务信息管理局2026年度局属政务信息系统运维项目的潜在投标人应在河南省公共资源交易中心（http://www.hnggzy.net）获取招标文件，并于2026年6月16日09时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-2026-526

2、项目名称：河南省行政审批和政务信息管理局2026年度局属政务信息系统运维项目

3、采购方式：公开招标

4、预算金额：17165200元

最高限价：17165200元

包号	交易编号	包名称	包预算（元）	包最高限价（元）
A包	豫政采(2)20260673-1	局属6个政务信息系统综合运维项目	10956700	10956700
B包	豫政采(2)20260673-2	省一体化政务服务平台（一期）子系统电子证照系统运维项目	800000	800000
C包	豫政采(2)20260673-3	省一体化协同办公平台运维项目	2479300	2479300
D包	豫政采(2)20260673-4	省电子政务外网管理中心（一期）运维项目	920000	920000
E包	豫政采(2)20260673-5	局属信息系统网络安全等级保护测评项目	440000	440000
F包	豫政采(2)20260673-6	局属信息系统密码应用安全性评估项目	192000	192000
G包	豫政采(2)20260673-7	局属信息系统综合安全监管项目	1377200	1377200
合计			17165200	17165200

5、采购需求（包括但不限于标的的名称、数量、简要技术需求或服务要求等）

5.1采购内容：

河南省行政审批和政务信息管理局2026年度局属政务信息系统运维项目主要包含：局属6个政务信息系统综合运维项目、省一体化政务服务平台（一期）子系统电子证照

系统运维项目、省一体化协同办公平台运维项目、省电子政务外网管理中心（一期）运维项目、局属信息系统网络安全等级保护测评项目、局属信息系统密码应用安全性评估项目和局属信息系统综合安全监管项目共7个包，详见招标文件第五章采购需求。

5.2 服务质量：满足行业标准和采购人要求；

5.3 服务地点：郑州市内采购人指定地点；

5.4 服务周期：自合同签订之日起1年。

6.合同履行期限：自合同签订之日起1年。

7.本项目是否接受联合体投标：否；

8.是否接受进口产品：否。

9.是否专门面向中小企业：否

二、申请人资格要求：

1、满足《中华人民共和国政府采购法》第二十二条规定；

2、落实政府采购政策满足的资格要求：/

3、本项目的特定资格要求

3.1 具有独立承担民事责任的能力；供应商是企业（包括合伙企业），应提供在市场监督管理局注册的有效“企业法人营业执照”或“营业执照”复印件或扫描件；供应商是事业单位，应提供有效的“事业单位法人证书”复印件或扫描件；

3.2 具有健全的财务制度，提供经审计的2024年或2025年度财务状况报告（公司成立年限不足的企业应提供其基本开户银行出具的资信证明）；

3.3 具有依法缴纳税收和社会保障资金的良好记录，提供2025年9月1日以来至少一个月的依法缴纳税收和社会保障资金的相关证明；

3.4 具有履行合同所必需的设备和专业技术能力，提供声明函；

3.5 具有良好的商业信誉，在参加本次政府采购活动前三年内，在经营活动中没有重大违法记录的书面声明或证明材料，提供声明函；

3.6 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。

3.7 根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》(财库[2016]125号)的规定，对列入失信被执行人、税收违法黑名单、政府采购严重违法失信行为记录名单的投标供应商，拒绝参与本项目政府采购活动。采购人或采购代理机构查询渠道：

失信被执行人查询渠道：“中国执行信息公开网”网站；

税收违法黑名单查询渠道：“信用中国”网站；

政府采购严重违法失信行为查询渠道：“中国政府采购网”。

三、获取招标文件

1、时间：2026 年 5 月 27 日至 2026 年 6 月 2 日，每天上午 00:00 至 12:00，下午 12:01 至 23:59（北京时间，法定节假日除外。）

2、地点：河南省公共资源交易中心（http://www.hnggzy.net）

3、方式：凭 CA 密钥登陆会员专区并在规定时间内按网上提示下载招标文件及资料（CA 密钥的办理及使用见河南省公共资源交易中心网站-公共服务-办事指南）

4、售价：0 元

四、投标截止时间及地点

1.时间：2026 年 6 月 16 日 09 时 00 分（北京时间）

2.地点:河南省公共资源交易中心（http://www.hnggzy.net）电子交易平台远程开标室(三)-2

五、开标时间及地点

1.时间：2026 年 6 月 16 日 09 时 00 分（北京时间）

2.地点：本项目采用不见面开标，供应商可不到开标现场解密。不见面服务的具体事宜请查阅河南省公共资源交易中心网站“公共服务-办事指南”专区的《新交易平台使用手册（培训资料）》。

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门户网》上发布。招标公告期限为五个工作日。

七、其他补充事宜

本项目需要优先落实的政府采购政策：

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.《政府采购促进中小企业发展管理办法》(财库〔2020〕46 号）；

4.《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）；

5.《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）。

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：河南省行政审批和政务信息管理局

地址：河南省郑州市金水区金水东路 22 号

联系人：祝斌

联系方式：0371-69698103

2.采购代理机构信息（如有）

名称：河南省机电设备招标股份有限公司

地址：郑州市商务外环路 23 号中科大厦 8 楼 824 室

联系人：王盼盼、周颖

联系方式：0371-65928756

3.项目联系方式

项目联系人：王盼盼、周颖

联系方式：0371-65928756

发布人：河南省机电设备招标股份有限公司

2026 年 5 月 25 日

第二章 投标人须知

投标须知前附表

序号	内 容	说明和要求
1.1	采购人	名称：河南省行政审批和政务信息管理局 地址：河南省郑州市金水区金水东路 22 号 联系人：祝斌 联系方式：0371-69698103
1.2	采购代理机构	名称：河南省机电设备招标股份有限公司 地址：郑州市商务外环路 23 号中科大厦 8 楼 824 室 联系人：王盼盼、周颖 联系方式：0371-65928756 邮箱：hn65928756@126.com
3	✱采购预算价	项目预算金额：17165200 元；最高限价 17165200 元 A 包:10956700 元 B 包:800000 元 C 包:2479300 元 D 包:920000 元 E 包:440000 元 F 包:192000 元 G 包:1377200 元 **投标人投标总报价超过最高限价的，其投标将被视为无效投标。**
3.3	构成招标文件的其他文件	招标文件的澄清、修改及有关补充通知为招标文件的有效组成部分
10.2	✱合同履行期限	自合同签订之日起 1 年。
14.1	✱投标有效期	自投标截止时间之日起 90 日历天。
15.1	投标文件签字或盖章要求	电子投标文件： 招标文件规定的应加盖公章的证明材料必须加盖供应商公章。所有要求加盖供应商公章的地方都应用供应商单位的 CA

		印章。所有要求法定代表人或其委托代理人签字的地方都应用法定代表人或其委托代理人的CA 印章(授权委托书中授权代表签字，可手写签字扫描上传）。
16.1	投标文件递交地点	河南省公共资源交易中心（http://www.hnggzy.net）电子交易平台
17.1	投标文件递交截止时间	详见公告
20.1	开标时间	同投标截止时间
20.2	开标地点	河南省公共资源交易中心远程开标室 河南省公共资源交易中心远程开标大厅 （http://www.hnggzy.net/BidOpening/bidopeninghallaction/hall/login）
23.1	评标委员会的组成	评标委员会构成：7 人，其中技术、经济类专家 5 人，采购人代表 2 人； 评标专家确定方式：开标前从河南省政府采购评标专家库中随机抽取方式确定。
27.1	资格审查	**在开标结束后，采购人或者采购代理机构应当对投标人资格进行审查。**
28	评标方法	综合评分法
30.1	推荐中标候选人的数量	3 名 各供应商均可同时参加本次采购 7 个包的投标，但只允许中一个包。评标委员会按从 A 包到 G 包顺序评审，例：在 A 包排名第一的候选人，B、C、D、E、F、G 包不再被推荐为中标候选人，以此类推。
30.2	是否授权评标委员会直接确定中标人	否
31.1	履约保证金	本项目不收取履约保证金
31.2	针对同一采购程序环节的质疑次数	一次性提出

34	授予合同	中标人在中标通知书发出后15日内与采购人签订合同。
其他事项		
37.1.1	信用记录的使用	**1.信用查询** 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，对列入失信被执行人、重大税收违法案件当事人名单（重大税收违法失信主体）、政府采购严重违法失信行为记录名单的供应商，拒绝参与本项目采购活动 **2.信用查询时间** 采购人或采购代理机构将在资格审查时查询投标人的信用记录,并将复查结果网页打印或拍照并存档。经查询之后，网站信息发生的任何变更均不再作为评审依据，供应商自行提供的与网站信息不一致的其他证明材料不作为评审依据。 **3.查询网站** “信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询相关主体信用记录
37.1.2	✱服务地点	详见第一章招标公告规定。
37.1.3	付款方式	按照合同执行
37.1.5	✱政府采购强制采购产品	1.如采购人所采购产品为《关于印发节能产品政府采购品目清单的通知》财库〔2019〕19号“节能产品政府采购品目清单”中政府强制采购节能产品的，投标人应提供有效期内的节能认证证书（认证机构：应符合《市场监管总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告》[2019年第16号]的“参与实施政府采购节能产品认证机构名录”），否则其投标将被认定为**投标无效**。 2.如采购人所采购产品属于信息安全产品的，根据《关于信息安全产品实施政府采购的通知》财库[2010]48号和国家质

		量监督检验检疫总局、国家认证认可监督管理委员会《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 号的规定，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**。 3.投标产品已列入《市场监管总局关于优化强制性产品认证目录的公告》【2020 年第 18 号】的产品必须提供通过国家 3C 认证的有关证明材料。
37.1.6	政府采购政策	**1.投标人所投标的均为小型和微型企业制造的产品，其投标价格给予 10%的扣除，用扣除后的价格参与评审。参加投标的小微企业，应当按照《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定提供《中小企业声明函》。** **所投小微企业产品报价=所投小微企业产品报价合计×（1-10%）** **注：（1）在政府采购活动中，供应商提供的货物、工程或者服务符合下列情形的，享受本办法规定的中小企业扶持政策：** **①在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受本办法规定的中小企业扶持政策。②规定依据本办法规定享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业；③明确采购标的对应的中小企业划分标准所属行业；** **（3）本采购标的所属行业为：软件和信息技术服务。（划定标准为：中小微企业划分按照《国家统计局关于印发<统计上大中小微型企业划分办法（2017）>的通知》国统字【2017】213 号文件及《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）规定的划分标准为依据。）** 2.根据《财政部、司法部关于政府采购支持监狱企业发展

		有关问题的通知》（财库[2014]68 号）规定，本项目支持监狱企业参与政府采购活动。监狱企业参加本项目采购时，须提供《监狱企业声明函》，视同小型、微型企业，享受评审中价格扣除等政府采购促进中小企业发展的政府采购政策，监狱企业属于小型、微型企业的，不重复享受政策。 3.根据《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）文件规定，本项目支持残疾人福利性单位参与政府采购活动。符合条件的残疾人福利性单位参加本项目采购时，应当提供本通知规定的《残疾人福利性单位声明函》，并对声明的真实性负责，视同小型、微型企业，享受评审中价格扣除等政府采购促进中小企业发展的政府采购政策，残疾人福利性单位属于小型、微型企业的，不重复享受政策。 4.根据政府采购政策，本项目如涉及到自主创新采购产品，应当采购由财政部会同科技部等部门制定的《政府采购自主创新产品目录》内的产品。
37.1.7	代理服务费	代理费收取标准为： 河南省招标投标协会[2023]002 号文件规定的“服务类型代理服务费收费标准”文件附表招标代理服务收费标准，代理机构向中标人按照中标金额收取。 支付时间：在发出中标通知书时 采购代理服务费收取信息： 单位名称：河南省机电设备招标股份有限公司 开户银行：建设银行郑州直属支行 银行账号：4100 1526 0100 5020 2373
37.1.8	知识产权	1.构成本招标文件各个组成部分的文件，未经采购人书面同意，投标人不得擅自复印和用于非本招标项目所需的其他目的。 2.投标报价应包括所有需要向其他方支付的知识产权费用。

		3.投标人应保证，采购人在中华人民共和国使用其提供的任何产品时，免受第三方提出的侵犯其专利权、商标权或其它知识产权的侵权指控，否则投标人应承担所有法律和经济责任，由此给采购人带来的损失全部由投标人承担。 4.本项目所产生的成果的知识产权归采购人所有，采购人具有对其的完全处置权。
37.1.9	特别提醒	1.采购人和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及答疑文件，以此编制投标文件。 **2.因河南省公共资源交易中心平台在开标前具有保密性，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自负。** 3.招标文件提及“复印件”的，投标人可提供原件扫描件或其复印件扫描件。
37.2	解释权	构成本招标文件的各个组成文件应互为解释，互为说明。如有不明确或不一致，构成合同文件组成内容的，以合同文件约定内容为准，且以合同条款约定的合同文件优先顺序解释；除招标文件中有特别规定外，仅适用于招标投标阶段的规定，按招标公告、投标人须知、评标办法、投标文件格式的先后顺序解释；同一组成文件中就同一事项的规定或约定不一致的，以编排顺序在后者为准；同一组成文件不同版本之间有不一致的，以形成时间在后者为准。按本款前述规定仍不能形成结论的，由采购人负责解释。
37.3	招标文件中的特殊符号标注	本招标文件中标注“✱”项为实质性要求或条款。
37.4	其他要求	/

本投标须知前附表是对投标人须知的具体补充和修改，如有矛盾，应以本前附表为准。

一、总　则

1、采购人、采购代理机构及投标人

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：是指集中采购机构或从事采购代理业务的社会中介机构。本项目的采购代理机构见投标须知前附表。

1.3 投标人（供应商）：是指响应招标、参加投标竞争的法人、其他组织或者自然人。

本项目的投标人须满足以下条件：

1.3.1 在中华人民共和国境内注册，能够独立承担民事责任的本国供应商。

1.3.2 具备《中华人民共和国政府采购法》第二十二条关于供应商的规定，遵守本项目采购人本级和上级财政部门政府采购的有关规定。

1.3.3 以招标文件规定的方式获得了本项目的招标文件。

1.3.4 符合投标须知前附表中规定的合格投标人的其他资格要求。

1.4 如投标须知前附表中允许联合体投标，对联合体规定如下：

1.4.1 两个及以上供应商可以组成一个投标联合体，以一个投标人的身份投标。

1.4.2 联合体各方均应符合本须知 1.3.2 规定。

1.4.3 采购人根据采购项目对投标人的特殊要求，联合体中至少应当有一方符合相关规定。

1.4.4 联合体各方应签订共同投标协议，明确约定联合体各方承担的工作和相应的责任，并将共同投标协议作为投标文件第一部分的内容提交。

1.4.5 大中型企业、其他自然人、法人或者非法人组织与小型、微型企业组成联合体共同参加投标，共同投标协议中应写明小型、微型企业的协议合同金额占到共同投标协议投标总金额的比例。

1.4.6 以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他供应商另外组成联合体参加本项目同一合同项下的投标，否则相关投标将被认定为投标无效。

1.4.7 对联合体投标的其他资格要求见投标须知前附表。

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。**

2、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

3、招标文件的构成

3.1 招标文件包括：

（1）招标公告；

（2）投标人须知；

（3）评标办法及标准；

（4）合同条款及格式；

（5）采购需求；

（6）投标文件格式；

（7）供应商须知前附表规定的其他材料。

3.2 投标人应认真阅读和充分理解招标文件中所有的内容。

3.3 除 3.1 内容外，采购人在提交投标文件截止时间前，以书面形式发出的对招标文件的澄清或修改内容，均为招标文件的组成部分，对采购人和投标人起约束作用。

3.4 投标人获取招标文件后，应仔细检查招标文件的所有内容，如有问题应在获得招标文件后及时向采购人提出，否则，由此引起的损失由投标人自己承担。投标人同时应认真审阅招标文件中所有的事项、格式、条款和规范要求等，若投标人的投标文件没有按招标文件要求提交全部资料，或投标文件没有对招标文件做出实质性响应，其风险由投标人自行承担，投标将被认定为**投标无效**。

4、投标费用

无论投标过程中的做法和结果如何，投标人自行承担所有与参加投标有关的全部费用。

5、招标文件的澄清与修改

5.1 采购人可主动地或在解答投标人提出的澄清问题时对招标文件进行澄清或修

改。采购代理机构将以发布澄清（更正）公告的方式，澄清或修改招标文件，澄清或修改内容作为招标文件的组成部分。

5.2 澄清或者修改的内容可能影响投标文件编制的，采购代理机构将以书面形式通知所有获取招标文件的潜在投标人，并对其具有约束力。投标人在收到上述通知后，应及时向采购代理机构确认。投标人未回复的，视同已知晓澄清或者修改的内容。

因潜在投标人原因或通讯线路故障导致通知逾期送达或无法送达的，由投标人自行承担。

6、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。

7、招标文件的约束力

投标人一旦下载了本招标文件并参加投标，则招标文件对采购人和投标人起约束作用。

三、投标文件的编制

8、投标的范围及标准

8.1 当项目分为多个包时,投标人可选择招标文件中的一个或几个分包进行投标,在投标须知前附表中对投标人投标包数另有规定的除外。

8.2 每个分包均是不可分割的整体,投标人应当对所投分包招标文件中“采购需求”所列的所有内容进行投标，如仅响应分包中的部分内容，其相应包投标将被认定为**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服务均应符合国家强制性标准。

9、投标语言及度量衡单位

9.1 投标人提交的投标文件以及投标人与代理机构就有关投标的所有往来函电均应使用简体中文。

9.2 除技术规格及要求另有规定外，投标文件所使用的计量单位均采用国家法定计量单位。

10、投标文件构成及编制

10.1 投标文件应包括但不限于下列内容:“第六章投标文件格式”包括的所有内容。

10.2 投标文件的编制

10.2.1 投标文件应按第六章“投标文件格式”使用河南省公共资源交易系统投标文件制作工具软件编制。其中，开标一览表在满足招标文件实质性要求的基础上，可以提出比招标文件要求更有利于采购人的承诺。

10.2.2 投标文件应当对招标文件有关交货期、质保期以及招标文件中标注“✱”项的内容作出实质性响应。

10.2.3 投标人编制投标文件时,具体事宜请查阅河南省公共资源交易中心网站办事指南栏目的《新交易平台使用手册（培训资料）》（http://www.hnggzy.net/ggfw/004003/20210909/834dab66-d4b5-4fde-b432-57f2a6cfbfed.html）。

10.2.4 投标货物资格文件

10.2.4.1 投标人必须提供有关投标货物符合招标文件要求的证明文件,这些文件可以是说明书、样本、检测报告、技术白皮书、产品彩页等；投标设备有强制性认证要求的，须提供设备的 3C 认证证书（如有）。

10.2.4.2 投标人必须对招标文件中货物的技术要求逐项、逐条明确答复；并认真、详细的填写“技术规格偏离表”，逐项、逐条说明响应或偏离情况。

10.2.4.3 投标人所投货物的所有部件均应为全新的、未使用过的新型合格产品。

10.2.4.4 投标人认为应对其设备的性能特点、优越性等有必要进行补充说明的内容。

11、投标文件格式

11.1 投标文件应包括本须知第 10 条中规定的全部内容，投标人提交的投标文件应当使用招标文件所提供的投标文件格式（**表格可以按同样格式扩展；未提供格式的由投标人自拟格式；标明“若有”的，由投标人视自身情况提供，非必须提供**）。

11.2 招标文件中的每个包，是项目招标不可拆分的最小投标单元，投标人必须按此所投包编制投标文件，提交相应的文件资料，拆分包进行投标将视为漏项或非实质性响应不予接受。

12、投标报价

12.1 投标人的投标报价应当包含满足本次招标全部采购需求所应提供的货物、伴随服务,以及货物验收合格正式交付使用前所发生的一切费用（包括税费、培训费、检验

费用等）投标人应结合自身条件，充分考虑本项目实际情况以及市场因素、现场环境因素、社会因素等各方面的风险因素，投标报价将被认为已综合考虑可能发生的全部不可预见的风险费用。中标人无权再以估计不足为由提出任何延长项目期限、增加价款或索赔等要求。

注：以上相关费用包含但不限于税费、内陆运输费、保险费和伴随服务费、相关售后服务费用、软件维护升级费用等，均由投标人承担，并计入投标报价。

12.2 每个投标人只允许有一个投标报价,采购人不接受有任何有选择性报价的投标，投标人报价不能超过采购人的预算价。

12.3 投标人的投标报价如有漏项，视为已经包含在投标报价内。

12.4 投标报价包含单价和合价，单价乘数量与合价不符时以单价为准修正合价，单价小数点明显错误的除外。数字表示的价格与文字表示的价格不一致时以文字表示的为准。如果单价、分项总价和投标总价之间有差异，评标时以单价为准。投标人应当无条件接受以其所报单价为基准的价格调整，否则其投标文件将被拒绝。

12.5 投标文件中凡是与“报价”、“金额”有关的条款，前后金额数应一致，不一致时以开标一览表中的金额为准。

12.6 投标人应考虑价格变化风险。

12.7 投标报价不得低于企业成本。

12.8 投标人除按评标委员会要求对其报价进行修正外,不得以任何理由在投标截止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,将被认定为**投标无效**。

12.9 投标人以人民币填报所有单价或价格，合同实施时亦以人民币支付。

12.10 本项目招标代理费由中标人支付。此费用由投标人综合考虑到投标报价中，不再单独列项。

13、投标保证金

根据河南省财政厅豫财购[2019]4 号文件规定，本项目不收取投标保证金。

14、投标有效期

14.1 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**。

14.2 在特殊情况下，采购人于原投标有效期满前，可向投标人提出延长投标有效期的要求。这种要求与答复均应采用书面形式。投标人可以拒绝采购人的这一要求而放弃中标，同意延长的投标人既不能要求也不允许修改投标文件。

15、投标文件签署

15.1 投标人应按本须知前附表规定的签字或盖章要求签署。

15.2 全套投标文件应采用不可拆分方式装订。任何行间插字、涂改或增删，必须由投标人法人代表或其委托代理人签字或盖章。

四、投标文件的递交

16、投标文件的递交

16.1 投标人应在规定的投标截止时间前上传加密的电子投标文件到系统指定位置。请投标人在上传时认真检查上传投标文件是否完整、正确。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技术联系。投标文件的递交地点见投标人须知前附表。

16.2 除投标人须知前附表另有规定外，投标人所递交的投标文件不予退还。

16.3 逾期送达的或者未送达指定地点的投标文件，采购人不予受理。

17、投标截止时间

17.1 投标文件的递交时间不得迟于“投标人须知前附表”中规定的截止时间，否则将不予接受。投标文件的递交见投标人须知前附表。

17.2 采购人可以通过修改招标文件延长投标截止日期。在此情况下，招标文件购买者和投标人的所有权利和义务以及投标人受制的截止日期均应以延长后新的截止日期为准。

18、迟交的投标文件

投标人在投标截止时间前未上传电子投标文件的将视为放弃投标。

19、投标文件的补充、修改和撤回

在规定的投标截止时间前，投标人可以多次修改或撤回已递交的投标文件，最终投标文件以投标截止时间前完成上传至河南省公共资源交易中心交易系统最后一份投标文件为准。

五、开标及资格审查

20、开标时间和地点

20.1 开标时间：见投标人须知前附表。

20.2 开标地点：河南省公共资源交易中心不见面开标大厅（http://hnsggzyjy.henan.gov.cn/BidOpening/）。

21、开标程序

21.1 本项目采用电子开标。到投标截止时间止，各投标人对电子投标文件进行解密。投标人在投标截止时间前未上传电子投标文件的将视为放弃投标。

主持人按下列程序进行开标：

（1）宣布开标纪律。

（2）公布在投标截止时间前递交投标文件的投标人名称。

（3）电子投标文件解密及导入。

（4）通过河南省公共资源交易中心系统进行唱标。

（5）开标结束。

注：投标人在投标文件解密环节 30 分钟内未完成电子投标文件解密的视同放弃投标，采购人或采购代理机构将退回其电子投标文件。

21.2 开标时，出现下列情况的，其投标将被拒绝：

（1）投标人未按河南省公共资源交易中心系统中规定的时间内解密投标文件的。

（2）投标人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，而导致解密失败的。

22、资格审查

22.1 公开招标采购项目开标结束后，由采购人或采购代理机构对投标人的资格进行审查。只有资格审查合格的投标人的投标文件才能被送达评标委员会评审，投标人有一项不符合的，其将不通过资格审查，资格审查标准如下：

序号	评审因素	评审标准
资格评审标准	独立承担民事责任的能力	供应商是企业（包括合伙企业），应提供在市场监督管理局注册的有效“企业法人营业执照”或“营业执照”复印件或扫描件；供应商是事业单位，应提供有效的“事业单位法人证书”复印件或扫描件；
	健全的财务制度	提供2024年度或2025年度经审计的财务报告(成立不足1年的提供基本开户银行出具的资信证明)。财务报告须具有注册会计师盖章和签字。
	依法缴纳税收和社保的良好记录	提供2025年9月1日以来至少一个月的依法缴纳税收和社会保障资金的相关证明复印件或扫描件。依法免税或不需要缴纳社会保障资金的供应商，应提供相应文件证明其依法免税或不需要缴纳社会保障资金。
	具备履约能力	提供具有履行合同所必需的设备和专业技术能力的书面声明(格式参考第六章投标文件格式）或证明材料的复印件或扫描件。
	良好的商业信誉	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记录的书面声明（格式参考第六章投标文件格式）
	无关联关系声明	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。（格式参考第六章投标文件格式）
	信用记录	采购代理机构在开标当日查询投标供应商未被列入失信执行人、税收违法黑名单、政府采购严重违法失信等信用记录。查询时将查询网页进行截图或打印，以作证据留存，内容要完整清晰。
	结　论	是否通过资格审查

22.2 合格投标人不足3家的，不再评标。

六、评标

23、评标及评标委员会的组成

23.1 评标工作由依法组建的评标委员会负责。评标委员会由技术、经济等方面的专家和采购人代表组成，具体人数见投标须知前附表。

23.2 评标专家从法定相关专家库中随机抽取产生。评标委员会主任由评标委员会成员选举产生，负责主持具体评标工作,采购人代表不得作为评标委员会主任。评标委员会根据有关法律法规和招标文件规定的方法和标准独立评标，负责完成评标的全过程直至向采购人推荐中标候选人。

24、评标过程的保密

24.1 评标将采取全封闭的方式（不向其他投标人公布、透露其价格等信息）。评标开始后，直至授予中标人合同为止，凡属于对投标文件的审查、澄清、评价和比较有关的资料，中标候选人的推荐情况及其他任何与评标有关的情况均应严格保密。

24.2 在评标过程中，如果投标人试图在投标文件审查、澄清、比较及授予合同等方面向采购人和评标委员会施加任何影响，都将会导致其投标文件被拒绝。

25、投标文件的澄清、说明或补正

25.1 对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者补正。但不得超出投标文件的范围或改变投标文件的实质性内容，也不得未经评标委员会允许主动提出澄清、说明或者补正。

25.2 投标人的澄清、说明或补正是投标文件的组成部分，取代投标文件中被说明或补正的部分。

25.3 投标人的澄清、说明或者补正应当采用书面形式，并加盖公章或者由法定代表人或其授权的代表签字。

26、投标文件中报价的修正

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。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照本办法第二十四条规定经投标人确认后产生约束力，投标人不确认的，其**投标无效**。

27、评标

27.1 评标程序：

（1）首先由评标委员会对所有资格审查合格的投标人投标文件进行符合性审查。

（2）通过符合性审查的投标人按照第三章评标方法及标准规定对投标人进行打分，按照得分进行排序，并向采购人推荐中标候选人。

27.2 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。

27.3 投标偏离

投标文件中存在对招标文件负偏离的，按照评标办法中的规定执行。

27.4 投标无效

在对投标文件进比较与评价之前，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。

评标委员会判断投标是否响应只根据招标文件要求和投标文件内容。

27.4.1 如发现下列情况之一的，其投标将被认定为投标无效：

（1）未按照招标文件规定要求签署、盖章的；

（2）投标有效期不满足招标文件要求；

（3）维保期不满足招标文件要求；

（4）投标报价超过本项目采购预算价；

（5）不满足招标文件标注“✱”项实质性条款的；

（6）投标人以他人的名义投标、串通投标的，其投标无效；

1）不同供应商的电子投标（响应）文件上传计算机的网卡 MAC 地址、CPU 序列号和硬盘序列号等硬件信息相同的；

2）不同供应商的投标（响应）文件由同一电子设备编制、打印加密或者上传；

3）不同供应商的投标（响应）文件由同一电子设备打印、复印；

4）不同供应商的投标（响应）文件由同一人送达或者分发，或者不同供应商联系人为同一人或不同联系人的联系电话一致的；

5）不同供应商的投标（响应）文件的内容存在两处以上细节错误一致；

6）不同供应商的法定代表人、委托代理人、项目经理、项目负责人等由同一个单位缴纳社会保险或者领取报酬的；

7）不同供应商投标（响应）文件中法定代表人或者负责人签字出自同一人之手；

8）其它涉嫌串通的情形。

9）不同供应商的投标文件机器码一致的；

(7)投标人提供虚假材料谋取中标的；

(8)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，并不能在评标现场合理的时间内提供书面说明及相关证明材料证明其报价合理性的；

(9)投标文件报价出现前后不一致时，投标人不确认修正的；

(10)投标文件含有采购人不能接受的附加条件的；

(11)属于招标文件规定的其他投标无效情形；

(12)法律、法规和招标文件规定的其他无效情形。

27.5 评标委员会判断投标文件的响应性仅基于投标文件本身，而不寻求外部的证据。未实质上响应招标文件要求的投标文件将被拒绝，投标人不得通过修正或撤销不符之处而使其投标成为实质上响应投标。

27.6 评标专家将允许修正投标文件中不构成重大偏离的、微小的、非正规的、不一致的或不规则的地方，但这些修改不能影响任何投标人竞争地位的公正性。

27.7 在评标过程中，凡遇到招标文件中无界定或界定不清、前后不一致使评委会意见有分歧且又难以协商一致的问题，均由评委会予以表决，获得半数以上同意的即为通过，未获得半数同意的即为否决。评标委员会发现招标文件存在歧义、重大缺陷导致评标工作无法进行，或者招标文件内容违反国家有关强制性规定的，应当停止评标工作，与采购人或者采购代理机构沟通并作书面记录。

28、评标方法及标准

详见第三章。

29、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（或最高限价）；

（4）因重大变故，采购任务取消的。

七、定标

30、确定中标人

30.1 评标委员会将根据评标标准，按投标须知前附表中规定的数量推荐中标候选人。

30.2 按投标须知前附表中规定是否由评标委员会直接确定中标人。

30.3 评标结束后，代理机构在 2 个工作日内将评审报告送采购人确认，采购人在收到评审报告后 5 个工作日内，从评审报告中推荐的中标候选人中确定中标人，经采购人书面确认后，中标结果将在发布招标公告的同一网站上进行公告，中标公告期限 1 个工作日。

31、告知招标结果

在公告中标结果的同时，采购人或者采购代理机构对未通过资格审查的投标人，告知其未通过的原因；采用综合评分法评审的，告知未中标人本人的评审得分与排序。

32、中标通知书

32.1 在公告中标结果的同时，采购人向中标人发出中标通知书。

32.2 中标通知书将作为进行合同谈判和签订的依据。

33、质疑的提出与接收

33.1 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。

33.2 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。

33.3 超出法定质疑期提交的质疑将被拒绝。

33.4 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。

33.5 投标人对质疑、投诉应当有明确的请求和必要的证明材料，并对质疑和投诉内容的真实性承担责任。

八、合同的授予

34、合同授予标准

34.1 本招标项目的合同将授予按本须知第 30 款所确定的中标人。

34.2 采购人将根据评标报告，确定排名第一的中标候选人为中标人。当确定中标的中标候选人放弃中标、因不可抗力提出不能履行合同的，采购人可以按评标委员会推荐的中标候选人顺序顺延至第二中标候选人或重新进行招标，如第二中标候选人也放弃中标、因不可抗力提出不能履行合同的的采购人可顺延至第三中标候选人或重新进行招标。评标委员会推荐中标候选人的人数见投标人须知前附表。

34.3 更改采购货物数量的权力

政府采购合同履行中，采购人需追加与合同标的相同的货物、工程或者服务的，在不改变合同其他条款的前提下，可以与供应商协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的百分之十。

34.4 中标人在中标通知书发出后 15 日内与采购人签订合同。

35、合同协议书的签订

35.1 签订合同后，采购人和中标人不得订立背离合同实质性内容的其他协议。招标文件、中标人的投标文件和澄清文件、中标通知书等文件资料，均应作为签约的合同文本的附件和基础。

35.2 中标人不按中标通知书规定的时间内与采购人订立合同,则采购人将取消其中标人资格，给采购人造成损失的，应当予以赔偿，同时依法承担相应法律责任。

35.3 中标人应当按照合同约定履行义务，完成中标项目，不得将中标项目转让(转包)给他人，中标项目是否分包根据采购人要求执行。

36、履约保证金

详见投标须知前附表 33.1 规定。

九、其他

37、其他事项

37.1 其他事项见投标须知前附表。

37.2 本招标文件解释权见投标须知前附表。

37.3 未尽事宜，按国家有关法律、法规执行。

第三章 评标方法及标准

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.《政府采购评审专家管理办法》；

5. 其他相关的法律法规、部门规章及规范性文件规定；

6. 本项目招标文件。

二、评标原则：客观、公正、审慎的原则；

三、**评标方法：**

本项目评标方法采用综合评分法，根据《中华人民共和国政府采购法实施条例》第三十四条 综合评分法，是指投标文件满足招标文件全部实质性要求且按照评审因素的量化指标评审得分最高的供应商为中标候选人的评标方法。

四、评标程序：

1.符合性审查工作

符合性审查是指评标委员会依据招标文件的规定，从商务和技术方面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。详见符合性审查表。

2.要求投标人对投标文件有关事项作出澄清或者说明

根据《关于推动解决政府采购异常低价问题的通知》（财库〔2026〕2号）规定，本次采购活动强化政府采购异常低价审查，在本次政府采购评审中出现下列情形之一的，评审委员会应当启动异常低价投标（响应）审查程序：

（1）投标（响应）报价低于全部通过符合性审查供应商投标（响应）报价平均值50%的，即投标（响应）报价<全部通过符合性审查供应商投标（响应）报价平均值×50%；

（2）投标（响应）报价低于通过符合性审查的次低报价供应商投标（响应）报价50%的，即投标（响应）报价<通过符合性审查的次低报价供应商投标（响应）报价×50%；

（3）投标（响应）报价低于采购项目最高限价45%的，即投标（响应）报价<采购项目最高限价×45%；

（4）评审委员会基于专业判断，认为供应商报价过低，有可能影响产品质量或者

不能诚信履约的其他情形。属于前述第 1 项至第 4 项情形的，评审委员会启动异常低价投标（响应）审查后，应当要求相关供应商在评审现场合理的时间内对投标（响应）价格作出解释，提供项目具体成本测算等与报价合理性相关的书面说明及必要的证明材料，包括但不限于原材料成本、人工成本、制造费用等，给予相关供应商的合理时间一般不少于 30 分钟。其中，属于第 3 项情形，供应商已随投标（响应）文件一并提交相关书面说明及必要的证明材料的，在评审现场可不再重复提交。评审委员会应依据专业经验，参考同类项目中标（成交）价格、类似产品市场价格水平、行业人工费用标准、国家有关部门指导行业协会发布的行业平均成本等情况，对报价合理性进行判断。投标（响应）供应商不能提供书面说明、证明材料，或者提供的书面说明、证明材料不能证明其报价合理性的，评审委员会应当将其作为无效投标（响应）处理。采购人、采购代理机构应当为评审委员会在评审现场及时获取同类项目中标（成交）价格、类似产品市场价格水平、行业人工费用标准、国家有关部门指导行业协会发布的行业平均成本等相关信息资料提供便利。评审委员会借助互联网等渠道查询相关信息的，应当严格遵守评审工作纪律，不得实施影响评审公正的行为。异常低价投标（响应）审查的启动原因、审查意见和审查结果应当在评审报告中记录，并随供应商提供的相关书面说明及证明材料，以及评审委员会有关互联网浏览、查询历史一并归档。

3. 对投标文件进行比较和评价

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，以评审因素的量化指标评审得分从高到低顺序确定中标候选人。

评标委员会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。

4. 检查复核评标结果。

5. 评标委员会根据全体评标成员签字的原始评标记录和评标结果编写评标报告。评标报告包括以下内容：

（一）招标公告刊登的媒体名称、开标日期和地点；

（二）投标人名单和评标委员会成员名单；

（三）评标方法和标准；

（四）开标记录和评标情况及说明，包括无效投标人名单及原因；

（五）评标结果，确定的中标候选人名单或者经采购人委托直接确定的中标人；

（六）其他需要说明的情况，包括评标过程中投标人根据评标委员会要求进行的澄清、说明或者补正，评标委员会成员的更换等。

五、评标纪律：

1.评标委员会成员应当按照评标原则，根据招标文件规定的评审程序、评审方法和评审标准进行评审。

2.与投标有利害关系的人员应当回避，不得进入评标委员会；

3.评标委员会成员在中标结果公告前，应对参与的评标委员会成员名单保密。

4.评标委员会成员应当在评审报告上签字，对自己的评审意见承担法律责任。对评审报告有异议的，应当在评审报告上签署不同意见，并说明理由，否则视为同意评审报告。

5.评标委员会及其成员不得有下列行为：

（一）确定参与评标至评标结束前私自接触投标人；

（二）除投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容外，接受投标人提出的与投标文件不一致的澄清或者说明；

（三）违反评标纪律发表倾向性意见或者征询采购人的倾向性意见；

（四）对需要专业判断的主观评审因素协商评分；

（五）在评标过程中擅离职守，影响评标程序正常进行的；

（六）记录、复制或者带走任何评标资料；

（七）其他不遵守评标纪律的行为。

评标委员会成员有前款第一至五项行为之一的，其评审意见无效。

六、评标标准：

评标委员会应当按照招标文件中规定的评标方法和标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价。

评标委员会应当按照符合性审查表对通过资格审查的投标人的投标文件进行评审，以确定其是否满足招标文件的实质性要求，有一项不满足的，其投标文件按无效标处理。审查标准见下表：

1、符合性审查表

序号	评审因素	评审标准

1	**形式评审标准**	投标人名称	与营业执照一致
		投标文件签字盖章	按照招标文件格式要求有法定代表人或其委托代理人签字或盖章、加盖单位公章
		报价唯一	只能有一个有效总报价
2	**响应性评审标准**	投标报价	未超过招标文件规定的最高限价
		投标范围	投标人对所投分包招标文件中所列的所有内容进行投标
		服务周期	符合招标文件要求
		质量要求	符合招标文件要求
		服务地点	符合招标文件要求
		投标有效期	符合招标文件要求
		实质性响应	满足本招标文件中标注“✱”项实质性条款
		标书雷同性分析	投标（响应）文件制作机器码不能一致

A 包:评分标准如下：

	分值构成	总分：100 分； 其中：投标报价：10 分 综合部分：25 分 技术部分：65 分	
序号	评审因素	评审因素量化指标	分值
1	投标报价 10 分	价格分采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算： 投标报价得分=(评标基准价/投标报价)×10 因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。具体规定如下： **中小企业产品价格给予扣除标准：** 1.根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，投标人提供由小微企业制造的产品的价格给予 10%的扣除，用扣除后的价格参与评审。对于所投产品中有大中型企业产品的价格不予扣除。投标人须提供《中小企业声明函（货物）》，否则不予认可。 2.根据财库〔2017〕141 号《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》，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除 10%等促进中小企业发展的政府采购政策。符合条件的残疾人福利性单位在参加政府采购活动时，应当提供本通知规定的《残疾人福利性单位声明函》，并对声明的真实性负责，不再提供《中小企业声明函（货物）》。中标、成交供应商为残疾人福利性单位的，采购人或者其委托的采购代理机构应当随中标、成交结果同时公告其《残疾人福利性单位声明函》，接受社会监督。 3.根据财库〔2014〕68 号《财政部司法部关于政府采购支持	10 分

			监狱企业发展有关问题的通知》，监狱企业视同小微企业。监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地(设区的市)监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业参加投标活动时，提供由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，不再提供《中小企业声明函（货物）》。在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除 10%等政府采购促进中小企业发展的政府采购政策。	
2	综合部分 25 分	业绩（6 分）	供应商提供 2023 年 1 月 1 日以来信息化运维服务项目相关业绩，每提供一份得 2 分，该项最多得 6 分。投标文件须提供合同原件扫描件、中标(成交)通知书原件扫描件，以合同签订时间为准，未按要求提供不得分；评标时每一份业绩须同时提供合同、中标/成交通知书及中标公告，不提供或提供不全者不得分。	6 分
		企业实力（5 分）	供应商具有以下有效证书的： 1. ISO9001 质量管理体系认证证书； 2. ISO27001 信息安全管理体系认证证书； 3. ISO20000 信息技术服务管理体系认证证书； 4. 信息技术服务运行维护标准符合性证书（ITSS）运行维护三级及以上； 5. 信息安全服务资质认证证书（信息系统安全运维）； 以上证书每提供 1 项得 1 分，该项最多得 5 分（提供相关证书扫描件或复印件加盖供应商公章）	5 分

		项目经理（6分）	项目经理具有计算机技术与软件专业技术资格（水平）考试信息系统项目管理师证书（高级）、系统集成项目管理工程师证书、具有中级及以上职称证书。每有一个证书得2分，最多得6分。 注:投标文件中须同时提供上述人员相关证书及供应商为其所缴纳的2026年以来不低于一个月的社保证明材料，并提供劳务合同关键信息页，缺项不得分。	**6分**
		运维人员配置方案（8分）	供应商按照项目运维人员配置及要求编写服务团队管理方案，包括：人数、人员结构、从业经验、技术资格证书、社保证明及劳动合同关键信息页、团队管理办法等。评标委员会根据投标文件此部分的响应情况进行评分： 1.提供人员配置方案完整且完全满足采购需求，服务团队管理方案与本项目需求完全匹配、详细完善，人员配比符合行业惯例，各岗位人员配比完全满足采购需求，人员数量充足，人员从业经验丰富满足业务量需求，有完整的技术资格证书、社保证明及劳动合同关键信息页完全满足招标文件要求的得8分； 2.提供人员配置方案合理，人员有相关从业经验，有技术资格证书、社保证明及劳动合同关键信息页，有基本的团队管理方案，基本满足招标文件采购需求的得5分； 3.提供人员配置方案有部分技术资格证书、社保证明及劳动合同关键信息页，有团队管理办法方案，但内容与本项目需求相比简略的得2分； 4.团队管理方案缺项，或不合理，或者不适用，不得分。 注： 1.人员配置团队中的所有成员须提供劳动合同关键信息页，并提供供应商为其所缴纳的2026年以来不低于一个月的社保证明材料，缺项不得分。 2.团队成员：拟派项目团队成员（项目经理除外），至少22名人员，每人须具有计算机技术与软件专业技术资格中级及	**8分**

			以上证书、或中级及以上职称证书、或中国信息安全测评中心颁发的注册信息安全专业人员证书，须提供证书扫描件，缺项不得分。	
3	技术部分(65分)	河南省一体化政务服务平台（一期)(除电子证照系统）方案（10分）	投标人针对本项目采购需求提供河南省一体化政务服务平台（一期）（除电子证照系统）服务方案，包括但不限于**基础环境及软件运维、业务系统运维、政务服务工单运维、短信服务平台运维、扫脸控件运维、用户信息核验、证书服务、安全运维**等服务内容。 1.运维服务方案完整且完全满足采购需求，基础环境及软件运维、业务系统运维、政务服务工单运维、短信服务平台运维、扫脸控件运维、用户信息核验、证书服务、安全运维服务内容完整齐全、详细全面且平台运维服务响应时效性高、系统优化服务完善、技术咨询专业高效的得10分； 2.运维服务方案基本符合需求，有基本的基础环境及软件运维、业务系统运维、政务服务工单运维、短信服务平台运维、扫脸控件运维、用户信息核验、证书服务、安全运维服务内容、运维服务方案、系统优化方案、技术咨询方案能基本满足采购需求的得6分； 3.运维服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得3分； 4.未提供得0分。	10分

		河南省政务服务移动端“豫事办”(一期)服务方案（9分）	投标人针对本项目采购需求提供河南省政务服务移动端“豫事办”(一期)服务方案，包括但不限于基础环境及软件运维、业务系统运维、安全运维等服务内容。 1.运维服务方案完整齐全且完全满足采购需求，基础环境及软件运维、业务系统运维、安全运维服务内容完整、详细全面且平台运维服务响应时效性高、应用优化服务方案完整、技术咨询专业高效的得9分； 2.运维服务方案基本符合采购需求，有基本的基础环境及软件运维、业务系统运维内容、安全运维服务、运维服务方案、应用优化服务方案、技术咨询方案的得6分； 3.运维服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得3分； 4.未提供得0分。	**9分**
		河南省“豫正通”服务方案（9分）	投标人针对本项目采购需求提供河南省“豫正通”服务方案，包括但不限于基础环境及软件运维、业务系统运维、安全运维等服务内容。 1.运维服务方案完整齐全且完全满足采购需求，基础环境及软件运维、业务系统运维、软硬件设备运维、安全运维服务内容非常完整、详细全面且平台运维服务响应时效性高、技术咨询专业高效的得9分； 2.运维服务方案基本符合采购需求，有基本的基础环境及软件运维、业务系统运维、软硬件设备运维、安全运维服务内容比较完善、运维服务方案、技术咨询方案的得6分； 3.运维服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得3分； 4.未提供得0分。	**9分**

		河南省“互联网+监管”系统（一期）方案（9分）	投标人针对本项目采购需求提供河南省“互联网+监管”系统（一期）服务方案，包括但不限于基础环境及软件运维、业务系统运维、安全运维等服务内容。 1.运维服务方案完整齐全且完全满足采购需求，基础环境及软件运维、业务系统运维、安全运维服务内容非常完整、详细全面且平台运维服务响应时效性高、系统优化服务非常完善、技术咨询专业高效的得9分； 2.运维服务方案基本符合采购需求，有基本的基础环境及软件运维、业务系统运维、安全运维服务内容比较完善、运维服务方案、系统优化方案、技术咨询方案的得6分； 3.运维服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得3分； 4.未提供得0分。	**9分**
		内容安全监测项目服务方案（9分）	投标人针对本项目采购需求提供内容安全监测项目服务方案，包括但不限于内容安全监测平台、告警研判处置、系统日常运维、平台配置管理、业务系统运维、安全运维等服务内容。 1.运维服务方案完整齐全且完全满足采购需求，安全监测平台、告警研判处置、系统日常运维、平台配置管理、业务系统运维、安全运维等内容非常完整、详细全面且平台运维服务响应时效性高、优化服务非常完善、技术咨询专业高效的得9分； 2.运维服务方案基本符合采购需求，有基本的安全监测平台、告警研判处置、系统日常运维、平台配置管理、业务系统运维、安全运维等内容、运维服务方案、优化方案、技术咨询方案的得6分； 3.运维服务方案部分符合需求，内容不完善的得3分； 4.未提供得0分。	**9分**

		安全防护项目服务方案（9分）	投标人针对本项目采购需求提供安全防护项目服务方案，包括但不限于硬件设备维保、软件维保、运维保障服务、远程技术支持、护网防守服务等服务内容。 1.运维服务方案完整齐全且完全满足采购需求，硬件设备维保、软件维保、运维保障服务、远程技术支持、护网防守服务内容非常完整、详细全面且平台运维服务响应时效性高、系统优化服务非常完善、技术咨询专业高效的得9分； 2.运维服务方案基本符合采购需求，有基本的硬件设备维保、软件维保、运维保障服务、远程技术支持、护网防守服务内容比较完善、运维服务方案、优化方案、技术咨询方案的得6分； 3.运维服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得3分； 4.未提供得0分。	**9分**
		应急保障方案（5分）	评标委员会根据供应商针对本项目的应急事件（包括安全事件、设备设施故障事件、灾害性事件以及其他事件）提供应急响应服务，制定应急保障方案，根据方案的先进性、实用性等因素综合比较进行打分： 1.应急方案切实可行、方案全面内容描述完整、可实施性强、反应迅速得5分； 2.应急方案较为可行，有基本应急方案，有基本描述应急内容的得3分； 3.应急方案较差、内容不完整、可实施性较差，存在缺陷的得1分； 4.未提供得0分。	**5分**
		保密措施（5分）	评标委员会根据供应商针对本项目提出的保密措施等内容进行综合比较打分： 1.保密措施内容完整全面、内容描述完整详实、保密性强且有全面应对方案的得5分； 2.有基本保密措施、有基本保密内容描述的得 3分；	**5分**

			3.保密措施内容不完整，存在漏洞的得 1 分； 4.未提供得 0 分。	

B 包:评分标准如下：

	分值构成	总分：100 分； 其中：投标报价：10 分 综合部分：20 分 技术部分：70 分	
序号	评审因素	评审因素量化指标	分值
1	投标报价 10 分	价格分采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算： 投标报价得分=(评标基准价/投标报价)×10 因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。具体规定如下： **中小企业产品价格给予扣除标准：** 1.根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，供应商提供由小微企业制造的产品的价格给予 10%的扣除，用扣除后的价格参与评审。对于所投产品中有大中型企业产品的价格不予扣除。投标人须提供《中小企业声明函（货物）》，否则不予认可。 2.根据财库〔2017〕141 号《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》，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除 10%等促进中小企业发展的政府采购政策。符合条件的残疾人福利性单位在参加政府采购活动时，应当提供本通知规定的《残疾人福利性单位声明函》，并对声明的真实性负责，不再提供《中小企业声明函（货物）》。中标、成交供应商为残疾人福利性单位的，采购人或者其委托的采购代理机构应当随中标、成交结果同时公告其《残疾人福利性单位声明函》，接受社会监督。 3.根据财库〔2014〕68 号《财政部司法部关于政府采购支	10 分

			持监狱企业发展有关问题的通知》，监狱企业视同小微企业。监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地(设区的市)监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业参加投标活动时，提供由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，不再提供《中小企业声明函（货物）》。在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除 10%等政府采购促进中小企业发展的政府采购政策。	
2	综合部分 20 分	业绩（6 分）	投标人提供 2023 年 1 月 1 日以来政务信息系统运维服务项目业绩，每提供一份得 2 分，该项最多得 6 分。投标文件须提供合同原件扫描件、中标(成交)通知书原件扫描件，以合同签订时间为准，未按要求提供不得分；评标时每一份业绩须同时提供合同、中标/成交通知书及中标公告，不提供或提供不全者不得分。	6 分
		企业实力（4 分）	投标人具有以下有效证书的： 1.信息技术服务运行维护标准符合性证书（ITSS）运行维护三级及以上； 2.信息系统安全运维、信息系统安全集成、软件安全开发方面的信息安全服务资质认证证书（CCRC），具备一级服务资质； 3.符合中国软件行业协会团体标准《软件服务商交付能力评估标准》（T/SIA009-2020），交付能力达到二级及以上。 4.具有符合《信息系统建设和服务能力评估体系能力要求》，能力达到良好级（CS3）或优秀级（CS4）。 以上证书每提供 1 项得 1 分，该项最多得 4 分（提供相关证书扫描件或复印件加盖供应商公章）	4 分
		项目经理（4	项目经理具有计算机技术与软件专业技术资格（水平）考试信息系统项目管理师证书（2 分）、取得系统架构设计师或系统	4 分

		分）	分析师证书（2 分）。满足一项得 2 分，最高得 4 分。 注:投标文件中须同时提供上述人员相关证书及供应商为其所缴纳的 2026 年以来不低于一个月的社保证明材料，并提供劳务合同关键信息页，缺项不得分。	
		运维人员配置方案（6 分）	投标人按照项目运维人员配置及要求编写服务团队管理方案，包括：人数、人员结构、从业经验、技术资格证书、社保证明及劳动合同关键信息页、团队管理办法等。评标委员会根据投标文件此部分的响应情况进行评分：每提供满足招标文件要求的一名拟派人员得 2 分，最多得 6 分。 注： 1.人员配置团队中的所有成员须提供劳动合同关键信息页，并提供供应商为其所缴纳的 2026 年以来不低于一个月的社保证明材料，缺项不得分。 2.团队成员：拟派项目团队成员（项目经理除外），不少于 3 人（其中驻场人员不少于 2 人），每人须具有计算机技术与软件专业技术资格中级及以上证书、或中级及以上职称证书、或中国信息安全测评中心颁发的注册信息安全专业人员证书，须提供证书扫描件，缺项不得分。	**6 分**
3	**技术部分（70 分）**	**基础设施运维服务方案（15 分）**	投标人针对本项目采购需求提供河南省一体化政务服务平台（一期）子系统电子证照系统基础设施运维服务方案，包括但不限于系统巡检与资源监控、资源优化与备份恢复等服务内容。 1.运维服务方案完整齐全且完全满足采购需求，系统巡检与资源监控、资源优化与备份恢复服务内容描述完整、详细全面且运维服务响应时效性高、技术咨询专业高效的得 15 分； 2.运维服务方案基本符合采购需求，有基本的系统巡检与资源监控、资源优化与备份恢复服务内容、运维服务方案、性能优化方案、技术咨询方案的得 10 分； 3.运维服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得 5 分；	**15 分**

			4.未提供得0分。	
		系统日常运维服务方案（15分）	投标人针对本项目采购需求提供河南省一体化政务服务平台（一期）子系统电子证照系统运维项目日常运维服务方案，包括但不限于基础环境及软件运维、安全运维、日常问题处理、新增需求处理以及配合完成网络安全等级保护测评等方面提出方案设计，根据投标人提供的日常运维服务方案内容进行综合评审。 1.运维服务方案完整齐全且完全满足采购需求，基础环境及软件运维、安全运维、日常问题处理、新增需求处理以及配合完成网络安全等级保护测评等方面提出方案设计内容描述完整、详细全面且运维服务响应时效性高、漏洞修复及时、日常问题处理高效、技术咨询专业高效的得15分； 2.运维服务方案基本符合采购需求，有基本的基础环境及软件运维、安全运维、日常问题处理、新增需求处理以及配合完成网络安全等级保护测评等方面提出方案设计服务内容，运维服务方案、漏洞修补方案、技术咨询方案的得10分； 3.运维服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得5分； 4.未提供得0分。	15分
		安全运维服务方案(10分)	投标人针对本项目采购需求提供河南省一体化政务服务平台（一期）子系统电子证照系统安全运维服务方案，包括但不限于漏洞修复与安全加固、应急响应与演练、账号权限管理与安全检查、重大节日保障运维等服务内容。 1.安全运维服务方案完整齐全且完全满足采购需求，日常安全监测、安全合规检查、上线前安全自查整改、安全体检、漏洞修复与安全加固、应急响应与演练、账号权限管理与安全检查、重大节日保障运维内容描述完整、详细全面且平台运维服务响应时效性高、性能优化服务全面、技术咨询专业高效的得10分； 2.安全运维服务方案基本符合采购需求，有基本的日常安全	10分

			监测、安全合规检查、上线前安全自查整改、安全体检、漏洞修复与安全加固、应急响应与演练、账号权限管理与安全检查、重大节日保障运维内容、运维服务方案、性能优化方案、技术咨询方案的得 6 分； 3. 安全运维服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得 3 分； 4. 未提供得 0 分。	
		新老共享交换平台切换方案（10 分）	投标人针对本项目采购需求提供河南省一体化政务服务平台(一期)子系统电子证照系统新老共享交换平台切换服务方案，包括但不限于库表数据迁移和共享接口切换等服务内容。 1. 新老共享交换平台切换方案完整齐全且完全满足采购需求，库表数据迁移和共享接口切换内容描述完整、详细全面且平台运维服务响应时效性高、性能优化服务全面、技术咨询专业高效的得 10 分； 2. 新老共享交换平台切换方案基本符合采购需求，有基本的库表数据迁移和共享接口切换内容、运维服务方案、性能优化方案、技术咨询方案的得 6 分； 3. 新老共享交换平台切换方案部分符合需求，有标题无实质性描述，方案存在缺陷的得 3 分； 4. 未提供得 0 分。	**10 分**
		系统迁移服务方案(10 分）	投标人针对本项目采购需求提供河南省一体化政务服务平台（一期）子系统电子证照系统迁移服务方案，包括但不限于系统迁移等服务内容。 1. 系统迁移服务方案完整齐全且完全满足采购需求，系统迁移内容描述完整、详细全面且运维服务响应时效性高、迁移适配度高、迁移系统运营稳定、技术咨询专业高效的得 10 分； 2. 系统迁移服务方案基本符合采购需求，有基本的系统迁移内容、有基本运维服务方案、迁移适配度适中、迁移系统能基本运营的得 6 分；	**10 分**

			3.系统迁移服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得3分； 4.未提供得0分。	
		应急保障方案（5分）	评标委员会根据供应商针对本项目的应急事件（包括安全事件、设备设施故障事件、灾害性事件以及其他事件）提供应急响应服务，制定应急保障方案，根据方案的先进性、实用性等因素综合比较进行打分： 1.应急方案切实可行、方案全面内容描述完整、可实施性强、反应迅速得5分； 2.应急方案较为可行，有基本应急方案，有基本描述应急内容的得3分； 3.应急方案较差、内容不完整、可实施性较差，存在缺陷的得1分； 4.未提供得0分。	**5分**
		保密措施（5分）	评标委员会根据供应商针对本项目提出的保密措施等内容进行综合比较打分： 1.保密措施内容完整全面、内容描述完整详实、保密性强且有全面应对方案的得5分； 2.有基本保密措施、有基本保密内容描述的得 3分； 3.保密措施内容不完整，存在漏洞的得 1分； 4.未提供得0分。	**5分**

C 包:评分标准如下：

	分值构成	总分：100 分； 其中：投标报价：10 分 综合部分：20 分 技术部分：70 分	
序号	评审因素	评审因素量化指标	分值
1	投标报价 10 分	价格分采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算： 投标报价得分=(评标基准价/投标报价)×10 因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。具体规定如下： **中小企业产品价格给予扣除标准：** 1.根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，供应商提供由小微企业制造的产品的价格给予 10%的扣除，用扣除后的价格参与评审。对于所投产品中有大中型企业产品的价格不予扣除。投标人须提供《中小企业声明函（货物）》，否则不予认可。 2.根据财库〔2017〕141 号《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》，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除 10%等促进中小企业发展的政府采购政策。符合条件的残疾人福利性单位在参加政府采购活动时，应当提供本通知规定的《残疾人福利性单位声明函》，并对声明的真实性负责，不再提供《中小企业声明函（货物）》。中标、成交供应商为残疾人福利性单位的，采购人或者其委托的采购代理机构应当随中标、成交结果同时公告其《残疾人福利性单位声明函》，接受社会监督。 3.根据财库〔2014〕68 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》，监狱企业视同小微企业。监	10 分

			狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地(设区的市)监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业参加投标活动时，提供由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，不再提供《中小企业声明函（货物）》。在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除 10%等政府采购促进中小企业发展的政府采购政策。	
2	综合部分20分	业绩（4分）	供应商提供 2023 年 1 月 1 日以来信息化建设或运维项目相关业绩，每提供一份得 2 分，该项最多得 4 分。投标文件须提供合同原件扫描件、中标(成交)通知书原件扫描件，以合同签订时间为准，未按要求提供不得分；评标时每一份业绩须同时提供合同、中标/成交通知书及中标公告，不提供或提供不全者不得分。	4分
		企业实力（4分）	供应商具有以下有效证书的： 1. ISO9001 质量管理体系认证证书； 2. ISO27001 信息安全管理体系认证证书； 3. ISO20000 信息技术服务管理体系认证证书； 4. 信息技术服务运行维护标准符合性证书（ITSS）运行维护三级及以上； 以上证书每提供 1 项得 1 分，该项最多得 4 分（提供相关证书扫描件或复印件加盖供应商公章）	4分
		项目经理（4分）	项目经理具有计算机技术与软件专业技术资格（水平）考试信息系统项目管理师证书（2 分）、计算机技术与软件专业技术资格（水平）考试系统架构设计师证书（2 分）。满足一项得 2 分，最高得 4 分。 注:投标文件中须同时提供上述人员相关证书及供应商为其所缴纳的 2026 年以来不低于一个月的社保证明材料，并提供劳	4分

			务合同关键信息页，缺项不得分。	
		运维人员配置方案（8分）	供应商按照项目运维人员配置及要求编写服务团队管理方案，包括：人数、人员结构、从业经验、技术资格证书、社保证明及劳动合同关键信息页、团队管理办法等。评标委员会根据投标文件此部分的响应情况进行评分：每提供满足招标文件要求的一名拟派人员得1.6分，最多得8分。 注： 1.人员配置团队中的所有成员须提供劳动合同关键信息页，并提供供应商为其所缴纳的2026年以来不低于一个月的社保证明材料，缺项不得分。 2.团队成员：拟派不少于5名驻场人员（项目经理除外），每人须具有计算机技术与软件专业技术资格中级及以上证书或中级及以上职称证书或中国信息安全测评中心颁发的注册信息安全专业人员证书，须提供证书扫描件，缺项不得分。	8分
3	技术部分(70分)	日常运维服务方案（15分）	投标人针对本项目采购需求提供省一体化协同办公平台的日常运维服务方案，包括但不限于基础环境及软件运维、安全运维、日常问题处理、新增需求处理以及配合完成网络安全等级保护测评及商用密码应用安全性评估工作等方面提供方案，根据投标人提供的日常运维服务方案内容进行综合评审。 1.运维服务方案完整齐全且完全满足采购需求，基础环境及软件运维、安全运维、日常问题处理、新增需求处理以及配合通过网络安全等级保护测评及商用密码应用安全性评估等方面提供的方案描述完整、详细全面且运维服务响应时效性高、漏洞修复及时、日常问题处理高效、技术咨询专业高效的得15分； 2.运维服务方案基本符合采购需求，有基本的基础环境及软件运维、安全运维、日常问题处理、新增需求处理以及配合通过网络安全等级保护测评及商用密码应用安全性评估等方面提供的方案内容、运维服务方案、漏洞修补方案、技术咨询方案的得10分；	15分

			3.运维服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得5分； 4.未提供得0分。	
		平台应用推广服务方案（15分）	投标人能够充分理解本项目平台应用推广服务要求，提供详细的平台应用推广服务方案，根据投标人提供的平台应用推广服务方案内容进行综合评审。 1.针对平台应用推广核心要求提供的详细方案，思路清晰完整、合理切实可行，方案完整齐全且完全满足采购需求的得15分。 2.能够提供基本的平台应用推广服务方案，方案思路基本清晰能基本符合采购需求的得10分。 3.提供的平台应用推广服务方案部分符合采购需求，有标题无实质性描述，方案存在缺陷的得5分。 4.未提供得0分。	**15分**
		系统对接服务方案（15分）	投标人能够充分理解本项目系统对接服务要求，提供详细的系统对接服务方案，根据投标人提供的系统对接服务方案内容进行综合评审。 1.针对各系统对接服务要求提供完整齐全且完全满足采购需求的系统对接服务方案，对接方式清晰完整、切实可行、方案描述详细的得15分。 2.能够提供基本符合采购需求的系统对接服务方案，有基本对接方式和针对性描述的得10分。 3.提供的系统对接服务方案部分符合采购需求，有标题无实质性描述，方案存在缺陷的5分。 4.未提供得0分。	**15分**

		项目实施方案（15分）	投标人需针对本项目实施要求所涉及的团队管理、服务报告与沟通机制、文档管理、保密管理、考核机制等内容来规划清晰、合理的方案。根据投标人提供的项目实施方案内容进行综合评审。 1.项目实施方案思路清晰完整，设计合理、切实可行的，有完整齐全管理机制、沟通机制、实施方案完整且完全满足采购需求的得15分。 2.项目实施方案基本符合采购需求，具有基本的实施方案和沟通管理机制的得10分。 3.方案内容部分符合采购需求，有标题无实质性描述，方案存在缺陷的5分。 4.未提供得0分。	**15分**
		应急保障方案（5分）	评标委员会根据供应商针对本项目的应急事件（包括安全事件、设备设施故障事件、灾害性事件以及其他事件）提供应急响应服务，制定应急保障方案，根据方案的先进性、实用性等因素综合比较进行打分： 1.应急方案切实可行、方案全面内容描述完整、可实施性强、反应迅速得5分； 2.应急方案较为可行，有基本应急方案，有基本描述应急内容的得3分； 3.应急方案较差、内容不完整、可实施性较差，存在缺陷的得1分； 4.未提供得0分。	**5分**
		保密措施（5分）	评标委员会根据供应商针对本项目提出的保密措施等内容进行综合比较打分： 1.保密措施内容完整全面、内容描述完整详实、保密性强且有全面应对方案的得5分； 2.有基本保密措施、有基本保密内容描述的得 3分； 3.保密措施内容不完整，存在漏洞的得 1分；	**5分**

			4.未提供得0分。	

D包:评分标准如下：

	分值构成	总分：100分； 其中：投标报价：10分 综合部分：20分 技术部分：70分	
序号	评审因素	评审因素量化指标	分值
1	投标报价 10分	价格分采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算： 投标报价得分=(评标基准价/投标报价)×10 因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。具体规定如下： **中小企业产品价格给予扣除标准：** 1.根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，供应商提供由小微企业制造的产品的价格给予10%的扣除，用扣除后的价格参与评审。对于所投产品中有大中型企业产品的价格不予扣除。投标人须提供《中小企业声明函（货物）》，否则不予认可。 2.根据财库〔2017〕141号《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》，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除10%等促进中小企业发展的政府采购政策。符合条件的残疾人福利性单位在参加政府采购活动时，应当提供本通知规定的《残疾人福利性单位声明函》，并对声明的真实性负责，不再提供《中小企业声明函	10分

			（货物）》。中标、成交供应商为残疾人福利性单位的，采购人或者其委托的采购代理机构应当随中标、成交结果同时公告其《残疾人福利性单位声明函》，接受社会监督。 3.根据财库〔2014〕68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》，监狱企业视同小微企业。监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地(设区的市)监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业参加投标活动时，提供由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，不再提供《中小企业声明函（货物）》。在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除10%等政府采购促进中小企业发展的政府采购政策。	
2	综合部分20分	业绩（4分）	供应商提供2023年1月1日以来信息化运维服务项目相关业绩，每提供一份得2分，该项最多得4分。投标文件须提供合同原件扫描件、中标(成交)通知书原件扫描件，以合同签订时间为准，未按要求提供不得分；评标时每一份业绩须同时提供合同、中标/成交通知书及中标公告，不提供或提供不全者不得分。	4分
		企业实力（4分）	供应商具有以下有效证书的： 1.ISO9001质量管理体系认证证书； 2.ISO27001信息安全管理体系认证证书； 3.ISO20000信息技术服务管理体系认证证书； 4.信息技术服务运行维护标准符合性证书（ITSS）运行维护三级及以上； 以上证书每提供1项得1分，该项最多得4分（提供相关证书扫描件或复印件加盖供应商公章）	4分
		项目经理	项目经理具有计算机技术与软件专业技术资格（水平）考试	3分

		（3 分）	信息系统项目管理师证书（1.5 分）、计算机技术与软件专业技术资格（水平）考试网络工程师或网络规划设计师证书（1.5 分）。满足一项得 1.5 分，最高得 3 分。 注:投标文件中须同时提供上述人员相关证书及供应商为其所缴纳的 2026 年以来不低于一个月的社保证明材料，并提供劳务合同关键信息页，缺项不得分。	
		运维人员配置方案（9 分）	供应商按照项目要求提供专职人员（不少于 4 人）、重保增配至少 2 人的服务团队管理方案，包括：人数、人员结构、从业经验、技术资格证书、社保证明及劳动合同关键信息页、团队管理办法等。评标委员会根据投标文件此部分的响应情况进行评分：每提供满足招标文件要求的一名拟派人员得 1.5 分，最多得 9 分。 注： 1.人员配置团队中的所有成员须提供劳动合同关键信息页，并提供供应商为其所缴纳的 2026 年以来不低于一个月的社保证明材料，缺项不得分。 2.团队成员：拟派项目团队成员（项目经理除外），至少 6 名人员，每人须具有计算机技术与软件专业技术资格中级及以上证书或中级及以上职称证书或中国信息安全测评中心颁发的注册信息安全专业人员证书，须提供证书扫描件，缺项不得分。	9 分
3	技术部分(70 分)	硬件维保服务方案（15 分）	投标人针对本项目采购需求提供河南省电子政务外网管理中心（一期）硬件维保服务方案，包括但不限于设备巡检、故障处理、漏洞修复、版本升级、安全设备特征库更新、设备保修及配件更换等服务内容 1.维保服务方案完整齐全且完全满足采购需求，设备巡检、故障处理、漏洞修复、版本升级、安全设备特征库更新、设备保修及配件更换等服务内容描述完整、详细全面且设备巡检、故障处理及时、版本升级更新高效、技术咨询专业高效的得 15 分；	15 分

			2.维保服务方案基本符合采购需求，有基本的设备巡检、故障处理、漏洞修复、版本升级、安全设备特征库更新、设备保修及配件更换等服务内容、运维服务方案、升级方案、技术咨询等方案的得10分； 3.维保服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的5分； 4.未提供得0分。	
		软件维保服务方案（15分）	投标人针对本项目采购需求提供河南省电子政务外网管理中心（一期）软件维保服务方案，包括但不限于各类型软件的故障处理、漏洞修复、版本升级、技术咨询等。 1.维保服务方案完整齐全且完全满足采购需求，各类型软件的故障处理、漏洞修复、版本升级、技术咨询等内容非常完整、详细全面且运维服务响应时效性高、版本升级服务非常完善、故障处理及时、漏洞修复及时、技术咨询专业高效的得15分； 2.维保服务方案基本符合采购需求，有基本各类型软件的故障处理、漏洞修复、版本升级、技术咨询内容、有基本运维服务方案、升级方案、技术咨询方案等得10分； 3.维保服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得5分； 4.未提供得0分。	**15分**
		运维保障服务方案（20分）	投标人针对本项目采购需求提供河南省电子政务外网管理中心（一期）运维保障服务方案，包括但不限于日常运维服务、信息资源维护、安全防护、重保期间运维保障服务、应急演练、护网防守服务、团队管理等服务内容。	**20分**

			1.运维保障服务方案完整齐全且完全满足采购需求、方案切实可行、可实施性强，方案完全满足运维服务场地要求、运维服务方式要求、运维服务响应要求的得20分； 2.运维保障服务方案基本符合采购需求，方案基本满足运维服务场地要求、运维服务方式要求、运维服务响应时限要求的得15分； 3.运维保障服务方案部分符合采购需求，有标题无实质性描述，方案存在缺陷的得8分； 4.未提供得0分。	
		应急保障方案（10分）	评标委员会根据供应商针对本项目的应急事件（包括安全事件、设备设施故障事件、灾害性事件以及其他事件）提供应急响应服务，制定应急保障方案，根据方案的先进性、实用性等因素综合比较进行打分： 1.应急方案切实可行、方案全面内容描述完整、可实施性强、反应迅速得10分； 2.应急方案较为可行，有基本应急方案，有基本描述应急内容的得6分； 3.应急方案较差、内容不完整、可实施性较差，存在缺陷的得3分； 4.未提供得0分。	**10分**
		保密措施（10分）	评标委员会根据供应商针对本项目提出的保密措施等内容进行综合比较打分： 1.保密措施内容完整全面、内容描述完整详实、保密性强且有全面应对方案的得10分； 2.有基本保密措施、有基本保密内容描述的得6分； 3.保密措施内容不完整，存在漏洞的得3分； 4.未提供得0分。	**10分**

E 包:评分标准如下：

	分值构成	总分：100 分； 其中：投标报价：10 分 综合部分：25 分 技术部分：65 分	
序号	评审因素	评审因素量化指标	分值
1	投标报价 10 分	价格分采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算： 投标报价得分=(评标基准价/投标报价)×10 因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。具体规定如下： **中小企业产品价格给予扣除标准：** 1.根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，供应商提供由小微企业制造的产品的价格给予 10%的扣除，用扣除后的价格参与评审。对于所投产品中有大中型企业产品的价格不予扣除。投标人须提供《中小企业声明函（货物）》，否则不予认可。 2、根据财库〔2017〕141 号《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》，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除 10%等促进中小企业发展的政府采购政策。符合条件的残疾人福利性单位在参加政府采购活动时，应当提供本通知规定的《残疾人福利性单位声明函》，并对声明的真实性负责，不再提供《中小企业声明函（货物）》。中标、成交供应商为残疾人福利性单位的，采购人或者其委托的采购代理机构应当随中标、成交结果同时公告其《残疾人福利性单位声明函》，接受社会监督。 3.根据财库〔2014〕68 号《财政部司法部关于政府采购支	10 分

			持监狱企业发展有关问题的通知》，监狱企业视同小微企业。监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地(设区的市)监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业参加投标活动时，提供由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，不再提供《中小企业声明函（货物）》。在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除10%等政府采购促进中小企业发展的政府采购政策。	
2	综合部分25分	业绩（6分）	投标人提供2023年1月1日以来省级政务信息化网络安全等级保护测评工作项目相关业绩，每提供一份得2分，该项最多得6分。投标文件须提供合同原件扫描件、中标(成交)通知书原件扫描件，以合同签订时间为准，未按要求提供不得分；评标时每一份业绩须同时提供合同、中标/成交通知书及中标公告，不提供或提供不全者不得分。	6分
		企业实力（7分）	投标人具有以下有效证书的： 1.ISO9001质量管理体系认证证书； 2.ISO27001信息安全管理体系认证证书； 3.ISO20000信息技术服务管理体系认证证书； 以上证书每提供1项得1分，该项最多得3分。（提供相关证书扫描件或复印件加盖投标人公章）	7分
			投标人具有中国信息安全测评中心颁发的安全工程、风险评估服务资质，每提供一项得2分，最多得4分。（提供相关证书扫描件或复印件加盖投标人公章）	
		项目经理(4分)	项目经理通过高级测评师认证且具备八年以上测评工作经验（以初次取得证书时间为准），具有网络安全服务能力评价证书CCSS-L，以上每具备一项加2分，最高得4分。	4分

		技术人员配备（8分）	拟派渗透测试人员 CISP-PTE（注册渗透测试工程师）具有中国信息安全测评中心颁发的CISP-CISI（注册信息安全讲师）认证得3分，不满足不得分。（提供相关证书扫描件或复印件加盖投标人公章） 拟派项目组技术人员不少于8人，其中： 具备高级网络安全等级测评师认证，每提供1人得0.5分，最多得3分。（提供相关证书扫描件或复印件加盖投标人公章） 具备中级网络安全等级测评师认证及CISAW（信息安全保障人员）认证，每提供1人得1分，最多得2分。（提供相关证书扫描件或复印件加盖投标人公章） 注：以上要求人员不得重复，重复人员不计分，人员配置中的所有成员须同时提供上述人员相关证书及劳动合同关键信息页，并提供投标人为其所缴纳的2026年以来不低于一个月的社保证明材料，缺项不得分。	8分
3	技术部分(65分)	测评方案（15分）	网络安全等级保护测评工作测评方案应综合考虑投标人方案编写的质量（方案包括但不限于项目需求分析、测评依据、工作原则、工具测试、安全整改建议、项目风险规避预测措施等），并对方案的合理性、可操作性、准确性等进行评价。 1.测评方案完整且完全满足采购需求，方案描述详细且针对性和可操作性强、准确性高的得15分 2.测评方案能基本满足采购需求，具有基本的网络安全等级保护测评工作测评方案得10分 3.测评方案有部分符合采购需求，标题无实质性描述，方案存在缺陷的得5分 4.未提供得0分。	15分
		安全检测能力（10分）	投标人每提供一项具有云环境数据资产漏洞扫描与防护类、中间件数据库巡查管理类、等保测评全生命周期管理类、安全配置核查类、邮件安全意识钓鱼平台类安全工具或专业技术证明，每提供一项得2分，最多得10分。须提供计算机软件	10分

			著作权登记证书。	
		项目实施计划与管理（10分）	投标方案中项目实施计划要求满足合理性及可操作性，对交流、实施、反馈及培训等相关环节进行安排： 1.项目实施计划与管理方案完整齐全且完全满足采购需求，人员分工明确、职责安排清晰，有详细的方案描述的得10分 2.项目实施计划与管理方案基本符合采购需求，有基本的项目实施计划与管理方案的得6分 3.项目实施计划与管理方案部分符合采购需求，有标题无实质性描述，方案存在缺陷的得3分。 4.未提供得0分。	**10分**
		风险管理与质量保障（10分）	投标人应该有明确的项目风险管理及质量保障措施，根据投标方案的可行性进行评审： 1.能结合本项目特点制定完全符合本项目的风险管理及质量保障措施，内容完整，描述详细得10分。 2.有基本的风险管理与质量保障基本能阐述但内容不具体的得6分 3.风险管理与质量保障措施有缺失、内容不完整或可行性一般的得3分 4.未提供得0分。	**10分**
		应急保障方案（10分）	评标委员会根据供应商针对本项目的应急事件（包括安全事件、设备设施故障事件、灾害性事件以及其他事件）提供应急响应服务，制定应急保障方案，根据方案的先进性、实用性等因素综合比较进行打分： 1.应急方案切实可行、方案全面内容描述完整、可实施性强、反应迅速得10分； 2.应急方案较为可行，有基本应急方案，有基本描述应急内容的得6分； 3.应急方案内容不完整、可实施性较差，存在缺陷的得3分； 4.未提供得0分。	**10分**

		保密措施（10分）	评标委员会根据供应商针对本项目提出的保密措施等内容进行综合比较打分： 1.保密措施内容完整全面、内容描述完整详实、保密性强且有全面应对方案的得10分； 2.有基本保密措施、有基本保密内容描述的得6分； 3.保密措施内容不完整，存在漏洞的得3分； 4.未提供得0分。	**10分**

F 包:评分标准如下：

	分值构成	总分：100 分； 其中：投标报价：10 分 综合部分：20 分 技术部分：70 分	
序号	**评审因素**	**评审因素量化指标**	**分值**
1	**投标报价 10 分**	价格分采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算： 投标报价得分=(评标基准价/投标报价)×10 因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。具体规定如下： **中小企业产品价格给予扣除标准：** 1.根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，供应商提供由小微企业制造的产品的价格给予 10%的扣除，用扣除后的价格参与评审。对于所投产品中有大中型企业产品的价格不予扣除。投标人须提供《中小企业声明函（货物）》，否则不予认可。 2.根据财库〔2017〕141 号《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》，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除 10%等促进中小企业发展的政府采购政策。符合条件的残疾人福利性单位在参加政府采购活动时，应当提供本通知规定的《残疾人福利性单位声明函》，并对声明的真实性负责，不再提供《中小企业声明函（货物）》。中标、成交供应商为残疾人福利性单位的，采购人或者其委托的采购代理机构应当随中标、成交结果同时公告其《残疾人福利性单位声明函》，接受社会监督。 3.根据财库〔2014〕68 号《财政部司法部关于政府采购支	**10 分**

			持监狱企业发展有关问题的通知》，监狱企业视同小微企业。监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地(设区的市)监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业参加投标活动时，提供由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，不再提供《中小企业声明函（货物）》。在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除 10%等政府采购促进中小企业发展的政府采购政策。	
2	综合部分 20 分	业绩（4 分）	投标人提供 2023 年 1 月 1 日以来省级政务信息化密码应用安全性评估工作项目相关业绩，每提供一份得 2 分，该项最多得 4 分。投标文件须提供合同原件扫描件、中标(成交)通知书原件扫描件，以合同签订时间为准，未按要求提供不得分；评标时每一份业绩须同时提供合同、中标/成交通知书及中标公告，不提供或提供不全者不得分。	4 分
		企业实力（4 分）	投标人具有以下有效证书的： 1. ISO9001 质量管理体系认证证书； 2. ISO27001 信息安全管理体系认证证书； 3. ISO20000 信息技术服务管理体系认证证书，认证方向为“商用密码应用安全性评估”相关； 4. 具有 CNAS 认证证书，认证方向为“商用密码应用安全性评估”； 以上证书每提供 1 项得 1 分，该项最多得 4 分（提供相关证书扫描件或复印件加盖投标人公章）	4 分
		项目经理（4 分）	项目经理通过商用密码应用安全性评估人员测评能力考核且具备八年以上测评经验（以取得证书的时间为准）；同时具备以下证书每有一项得 2 分，不满足不得分。	4 分

			1.具有信息系统项目管理师证书； 2.具备注册密码安全专业人员证书（NSATP-CSP） 注:投标文件中须同时提供上述人员相关证书及投标人为其所缴纳的2026年以来不低于一个月的社保证明材料，并提供劳务合同关键信息页，缺项不得分。	
		技术人员配备（8分）	拟派技术负责人通过商用密码应用安全性评估人员测评能力考核且具备五年以上测评经验（以取得证书的时间为准）、信息安全保障人员（CISAW）认证考核证书和注册信息安全工程师（CISP）认证考核证书，同时满足得4分，不满足不得分。（提供相关证书扫描件或复印件加盖投标人公章） 拟派项目组技术人员通过商用密码应用安全性评估人员测评能力考核且具备三年以上测评经验（以取得证书的时间为准），提供1人得1分，最多得4分。（提供相关证书扫描件或复印件加盖投标人公章） 注： 人员配置中的所有成员须同时提供上述人员相关证书及劳动合同关键信息页，并提供供应商为其所缴纳的2026年以来不低于一个月的社保证明材料，缺项不得分。	**8分**
3	**技术部分(70分)**	**评估服务方案（15分）**	投标人针对本项目采购需求提供河南省“豫正通”、河南省大数据中心(一期)、河南省一体化协同办公平台等3个系统的密码应用安全性评估工作服务方案，包括但不限于物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密码算法、密码技术、密码产品、密码服务、安全管理相关文档等评估服务内容。 1.评估服务方案完整且完全满足采购需求，物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密码算法、密码技术、密码产品、密码服务、安全管理相关文档服务内容完整齐全、详细全面且评估方案全面、严谨、专业高效的得	**15分**

			15 分； 2.评估服务方案基本符合需求，物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密码算法、密码技术、密码产品、密码服务、安全管理相关文档服务内容能基本满足采购需求、有基本的评估服务方案、技术咨询方案的得 10 分； 3.评估服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得 5 分； 4.未提供得 0 分。	
		通用要求评估服务方案（15 分）	投标人针对本项目采购需求提供河南省“豫正通”、河南省大数据中心(一期)、河南省一体化协同办公平台等 3 个系统的密码应用安全性评估工作通用要求服务方案，包括但不限于密码算法测评、密码技术测评、密码产品测评、密码服务测评等服务内容。 1.通用要求评估服务方案完整且完全满足采购需求，业务支撑与功能维护、数据处理与统计分析、工单处理与故障响应、运维报告与巡检记录内容完整齐全、详细全面且通用要求评估服务方案完整齐全、详细全面且评估方案全面、严谨、专业高效的得 15 分； 2.通用要求评估服务方案基本符合需求，有基本的业务支撑与功能维护、数据处理与统计分析、工单处理与故障响应、运维报告与巡检记录内容能基本满足采购需求、有基本通用要求评估服务方案、技术咨询方案的得 10 分； 3.通用要求评估服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得 5 分；	**15 分**

			4.未提供得0分。	
		网络和通信安全测评服务方案（10分）	投标人针对本项目采购需求提供河南省“豫正通”、河南省大数据中心(一期)、河南省一体化协同办公平台等3个系统的密码应用安全性评估工作的网络和通信安全测评服务方案，包括但不限于身份鉴别、通信数据完整性、重要数据的机密性、网络边界访问控制信息的完整性、安全接入认证、密码服务、密码产品等服务内容。 1.网络和通信安全测评服务方案完整且完全满足采购需求，身份鉴别、通信数据完整性、重要数据的机密性、网络边界访问控制信息的完整性、安全接入认证、密码服务、密码产品内容完整齐全、详细全面且网络和通信安全测评服务方案完整、描述详细全面且评估方案全面、严谨、专业高效的得10分； 2.网络和通信安全测评服务方案基本符合需求，漏洞修复与安全加固、应急响应与演练、账号权限管理与安全审计、重大节日保障运维内容能基本满足采购需求、有基本的网络和通信安全测评服务方案、技术咨询方案的得6分； 3.网络和通信安全测评服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得3分； 4.未提供得0分。	10分
		设备和计算安全测评方案（10分）	投标人针对本项目采购需求提供河南省“豫正通”、河南省大数据中心(一期)、河南省一体化协同办公平台等3个系统的密码应用安全性评估工作的设备和计算安全测评服务方案，包括但不限于身份鉴别、远程管理通道安全、访问控制信息完整性、重要信息资源安全标记完整性、日志记录完整性、重要可执行程序	10分

			完整性、重要可执行程序来源真实性、密码服务、密码产品等服务内容。 1.设备和计算安全测评服务方案完整且完全满足采购需求，身份鉴别、远程管理通道安全、访问控制信息完整性、重要信息资源安全标记完整性、日志记录完整性、重要可执行程序完整性、重要可执行程序来源真实性、密码服务、密码产品内容完整、内容描述详细全面、技术咨询专业高效的得10分； 2.设备和计算安全测评服务方案基本符合需求身份鉴别、远程管理通道安全、访问控制信息完整性、重要信息资源安全标记完整性、日志记录完整性、重要可执行程序完整性、重要可执行程序来源真实性、密码服务、密码产品内容能基本满足采购需求、有基本的设备和计算安全测评服务方案、技术咨询方案的得6分； 3.设备和计算安全测评服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得3分； 4.未提供得0分。	
		应用和数据安全测评服务方案（10分）	投标人针对本项目采购需求提供河南省“豫正通”、河南省大数据中心(一期)、河南省一体化协同办公平台等3个系统的应用和数据安全测评服务方案，包括但不限于身份鉴别、访问控制信息完整性、重要信息资源安全标记完整性、重要数据传输机密性、重要数据存储机密性、重要数据传输完整性、重要数据存储完整性、不可否认性、密码服务、密码产品等服务内容。 1.应用和数据安全测评服务方案完整且完全满足采购需求，身份鉴别、访问控制信息完整性、重要信息资源安全标记完整性、	**10分**

			重要数据传输机密性、重要数据存储机密性、重要数据传输完整性、重要数据存储完整性、不可否认性、密码服务、密码产品内容描述详细全面的得 10 分； 2. 应用和数据安全测评服务方案基本符合需求，身份鉴别、访问控制信息完整性、重要信息资源安全标记完整性、重要数据传输机密性、重要数据存储机密性、重要数据传输完整性、重要数据存储完整性、不可否认性、密码服务、密码产品内容有基本完整性和机密性的得 6 分； 3. 应用和数据安全测评服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得 3 分； 4. 未提供得 0 分。	
		测评工具（5 分）	投标人拥有自主知识产权的密码测评工具，每 4 个得 1 分，不足 4 个不计分，最多得 5 分。软著名称需含有“密码测评”或“密码评估”的字样，否则不得分。（提供软件著作权证书复印件并加盖供应商公章）。	**5 分**
		保密措施（5 分）	评标委员会根据供应商针对本项目提出的保密措施等内容进行综合比较打分： 1. 保密措施内容完整全面、内容描述完整详实、保密性强且有全面应对方案的得 5 分； 2. 有基本保密措施、有基本保密内容描述的得 3 分； 3. 保密措施内容不完整，存在漏洞的得 1 分； 4. 未提供得 0 分。	**5 分**

G 包:评分标准如下：

	分值构成	总分：100 分； 其中：投标报价：10 分 综合部分：15 分 技术部分：75 分	
序号	评审因素	评审因素量化指标	分值
1	投标报价 10 分	价格分采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算： 投标报价得分=(评标基准价/投标报价)×10 因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。具体规定如下： **中小企业产品价格给予扣除标准：** 1.根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，供应商提供由小微企业制造的产品的价格给予 10%的扣除，用扣除后的价格参与评审。对于所投产品中有大中型企业产品的价格不予扣除。投标人须提供《中小企业声明函（货物）》，否则不予认可。 2.根据财库〔2017〕141 号《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》，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除 10%等促进中小企业发展的政府采购政策。符合条件的残疾人福利性单位在参加政府采购活动时，应当提供本通知规定的《残疾人福利性单位声明函》，并对声明的真实性负责，不再提供《中小企业声明函（货物）》。中标、成交供应商为残疾人福利性单位的，采购人或者其委托的采购代理机构应当随中标、成交结果同时公告其《残疾人福利性单位声明函》，接受社会监督。 3.根据财库〔2014〕68 号《财政部司法部关于政府采购支	10 分

			持监狱企业发展有关问题的通知》，监狱企业视同小微企业。监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地(设区的市)监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业参加投标活动时，提供由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，不再提供《中小企业声明函（货物）》。在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除 10%等政府采购促进中小企业发展的政府采购政策。	
2	综合部分 15 分	业绩（4 分）	投标人提供 2023 年 1 月 1 日以来政务行业综合性安全服务案例，需含有“安全漏洞复测、上线检测评估、网络安全专项检查、安全风险评估、渗透测试、代码审计、个人信息安全合规评估、数据安全运营、漏洞扫描、安全应急响应、安全监测服务、应急演练”上述任意两个及以上组合关键词，每提供一份得 2 分，该项最多得 4 分。投标文件须提供合同原件扫描件、中标(成交)通知书原件扫描件，以合同签订时间为准，未按要求提供不得分；评标时每一份业绩须同时提供合同、中标/成交通知书及中标公告，不提供或提供不全者不得分。	4 分
		企业实力（4 分）	投标人具有以下有效证书的： 1. ISO9001 质量管理体系认证证书； 2. ISO27001 信息安全管理体系认证证书； 3. ISO20000 信息技术服务管理体系认证证书； 4. ISO28000 供应链安全管理体系； 以上证书每提供 1 项得 1 分，该项最多得 4 分（提供相关证书扫描件或复印件加盖投标人公章）	4 分
			项目经理具有计算机技术与软件专业技术资格（水平）考试信息系统项目管理师证书且具备八年以上经验（以取得证书的时	

		项目经理（2分）	间为准)、信息安全保障人员认证证书-风险管理专业级(CISAW)，每具备一项得1分，最多得2分。 注:投标文件中须同时提供上述人员相关证书及投标人为其所缴纳的2026年以来不低于一个月的社保证明材料，并提供劳务合同关键信息页，缺项不得分。	2分
		技术人员配备（5分）	拟派技术负责人具备注册信息安全工程师（CISP）认证考核证书、注册信息安全人员渗透测试专家（CISP-PTS），每具备一项得0.5分，最多得1分。 拟派项目组技术人员具备注册信息安全工程师（CISP）认证考核证书，每提供1名得1分，最多得4分。 注：人员配置中的所有成员须同时提供上述人员相关证书及劳动合同关键信息页，并提供投标人为其所缴纳的2026年以来不低于一个月的社保证明材料，缺项不得分。	5分
3	技术部分(75分)	综合安全监管服务方案（30分）	投标人针对本项目采购需求提供河南省一体化政务服务平台（一期）、河南省政务服务移动端“豫事办”(一期)、河南省“豫正通”、河南省“互联网+监管”系统（一期）、河南省一体化协同办公平台、河南省电子政务外网管理中心（一期）、安全防护项目、内容安全监测项目等综合安全监管服务方案，包括但不限于常态化渗透测试服务、上线前安全检查服务、安全审计服务、风险评估服务、安全漏洞复测服务、专项安全检查服务、安全应急响应服务、安全咨询服务等服务内容。 1.综合安全监管服务方案完整且完全满足采购需求，常态化渗透测试服务、上线前安全检查服务、安全审计服务、风险评估服务、安全漏洞复测服务、专项安全检查服务、安全应急响应服务、安全咨询服务服务内容完整齐全、详细全面且方案全面、严谨、逻辑性强、咨询专业高效的得30分； 2.综合安全监管服务方案基本符合需求，有基本的常态化渗透测试服务、上线前安全检查服务、安全审计服务、风险评估服务、安全漏洞复测服务、专项安全检查服务、安全应急响应服务、	30分

			安全咨询服务内容、有基本的检测服务方案、技术咨询方案的得20分； 3.综合安全监管服务方案部分符合需求，有标题无实质性描述，方案存在缺陷的得10分； 4.未提供得0分。	
		项目实施难点及关键过程分析（15分）	投标人针对本项目采购需求分析河南省一体化政务服务平台（一期）、河南省政务服务移动端“豫事办”(一期)、河南省“豫正通”、河南省“互联网+监管”系统（一期）、河南省一体化协同办公平台、河南省电子政务外网管理中心（一期）、安全防护项目、内容安全监测项目等综合安全监管服务中的关键和重难点。 1.项目实施难点及关键过程分析较透彻、方案完整且完全满足采购需求、过程控制较得当且有优秀的解决方案的得15分； 2.项目实施难点及关键过程分析能基本满足采购需求，并且有良好解决方案的得10分。 3.项目实施难点及关键过程分析不够透彻、方案存在缺陷的、过程控制不够得当的得5分； 4.未提供得0分。	**15分**
		服务质量保证体系与措施（15分）	投标人应该有明确的项目风险管理及质量保障措施，根据投标方案的可行性进行评审： 1.能结合本项目特点制定完全符合本项目的风险管理及质量保障措施，内容完整，描述详细得15分。 2.有基本的风险管理与质量保障有基本内容阐述但内容不具体的得10分。 3.风险管理与质量保障措施有缺失、内容不完整或可行性一般的得3分。 4.未提供得0分。	**15分**
			为确保安全服务过程中安全检测工具安全可靠，投标人须提供具有自主知识产权的商用安全检测工具，包括源代码审计、开	

		安全检测工具（5分）	源组件检测、自动化渗透测试（非漏洞扫描系统）、威胁情报系统、安全有效性验证评估、网络安全事件应急处置等工具，每提供1个得1分，最多得5分。（提供软件著作权证书，或网络关键设备和网络安全专用产品安全认证证书，或网络安全专用产品安全检测证书复印件并加盖投标人公章）	**5分**
		应急保障方案（5分）	评标委员会根据供应商针对本项目的应急事件（包括安全事件、设备设施故障事件、灾害性事件以及其他事件）提供应急响应服务，制定应急保障方案，根据方案的先进性、实用性等因素综合比较进行打分： 1.应急方案切实可行、方案全面内容描述完整、可实施性强、反应迅速得5分； 2.应急方案较为可行，有基本应急方案，有基本描述应急内容的得3分； 3.应急方案较差、内容不完整、可实施性较差，存在缺陷的得1分； 4.未提供得0分。	**5分**
		保密措施（5分）	评标委员会根据供应商针对本项目提出的保密措施等内容进行综合比较打分： 1.保密措施内容完整全面、内容描述完整详实、保密性强且有全面应对方案的得5分； 2.有基本保密措施、有基本保密内容描述的得 3分； 3.保密措施内容不完整，存在漏洞的得 1分； 4.未提供得0分。	**5分**

注：1、以上各评分项，若有缺项则该项不得分。

2、分值计算保留小数点后两位，第三位四舍五入。

七、落实的政府采购政策：

1.根据《政府采购促进中小企业发展管理办法》（财库[2020]46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《中小企业声明函》、《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10%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。

2.国家相关部委针对节能产品、环境标志产品出台了相关调整优化政府采购执行机制，并于近日相继颁布《财政部发展改革委 生态环境部 市场监管总局 关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）、《市场监管总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告》（市场监管总局2019年4月3日下发）（以下简称“机构名录”）、《关于印发节能产品政府采购品目清单的通知》（财库〔2019〕19号）（以下简称“节能清单”）、《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）（以下简称“环保清单”）。

根据要求，投标产品中如有属于“节能清单”中标记“★”产品的，必须提供经过“机构名录”中的认证机构出具的“节能产品认证证书”，未提供的按无效投标处理。

对于投标产品属于“节能清单”中非标记“★”产品的以及属于 “环保清单”产品并经“机构名录”中的认证机构出具相应的产品认证证书的每发生一项给予该项报价2%的扣除体现。

采购人采购产品属于节能产品或环境标志产品品目清单范围内，且投标人所投产品具有有效期内的产品认证证书，在评标时予以优先采购，具体优惠措施为：如果采购项目包有多种设备，每发生一项给予该项报价2%的扣除体现。

3.投标人所投产品列入“财政部国家发展改革委信息产业部关于印发无线局域网产品政府采购实施意见的通知财库［2005］366号”无线局域网产品清单，应提供相关证明，在评标时予以优先采购，具体优惠措施为：如果采购项目包有多种设备，每发生一项给予该项报价2%的扣除体现。

4.根据“关于信息安全产品实施政府采购的通知财库[2010]48号”要求，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无效投标。

八、评标时，特殊情况的处理原则：

1、得分并列时的处理原则

如出现中标候选人最终得分并列情况时，评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的，按技术标得分由高到低顺序排列。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。

第四章 合同条款及格式

河南省行政审批和政务信息管理局运维服务合同
（A 包、B 包、C 包、D 包）
（示范文本）

项目名称：20XX 年 XXXXXXXXX 运行维护项目

委托方（甲方）：_____

受托方（乙方）：_____

签订时间：_____

签订地点：_____

局属6个政务信息系统综合运维
服务合同

甲方：

乙方：

根据《中华人民共和国民法典》《中华人民共和国政府采购法》等规定，就_____（以下简称“乙方”）向河南省行政审批和政务信息管理局（以下简称“甲方”）提供_____（项目名称）事宜，双方经过平等协商，在真实、充分地表达各自意愿的基础上，达成如下协议，并由双方共同恪守。

第一条　相关术语的定义和解释

（一）定义

1．本项目：_____。

2．甲方：本项目甲方。

3．乙方：本项目成交服务商。

4．双方：指甲方和乙方。

5．合同：指双方就本项目达成并签署的协议，以及下面条款所列出的构成合同的所有文件。

6．甲方用户单位：指本合同所属项目甲方所涉及或授权管理的单位。

7．用户文档集：能够指导、帮助用户实施运维的所有文档的集合。除源代码外，服务过程中的产出物都属于用户文档集。

8．交付物：指乙方根据本合同规定须向甲方提供的一切文档、数据，以及为完成本项目用甲方资金采购的工具软件和系统软件等。

9．现场服务：指乙方根据合同约定义务派遣服务人员到甲方或甲方用户单位现场进行运维服务和解决问题的过程。

10．秘密：指甲方所拥有的，不为公众所知的管理信息、方式方法、用户名单、数据、信息、技术诀窍、源代码、计算机文档等，或由双方在履行本合同过程中明确指明为秘密的、法律所认可的任何信息。

（二）解释

1．“年、月、日、天、周”：分别是公历的年、月、日、周；00:00:00至23:59:59为整天；周：是指周一到周日完整7天。

2．“工作日”：是指国家所规定的节假日之外的所有的工作日。

3．“自然日”：指一天24小时，包括正常的工作日和节假日。

4．“不可抗力”：是指双方在缔结合同时所不能预见的、并且其发生及后果是无法避免和无法克服的客观情况。

5．“元”：是指人民币元。

6．“条款或附件”：指本合同的条款或附件。

7．除本合同另有明确约定，“包括”指包括但不限于；除本合同另有明确约定，“以上”“以下”“以内”或“内”均含本数，“超过”“以外”不含本数。

第二条　承诺和保证

（一）甲方的承诺和保证

1．在本合同生效日前已获得了签订本合同所必需的授权，有权签署本合同。

2．甲方为签署本合同已经依据甲方政府采购之规定完成所有必要的内部行为，其有权签署本合同并履行本合同项下的义务。

3．如果甲方的保证被证明在工作时存在不实或不能兑现，对乙方依本合同享有权利或承担义务造成实质性影响时，乙方有权提前终止本合同，并依据影响程度进行追责、追偿，本合同各附件也随之自动终止。

（二）乙方的承诺和保证

1．乙方是依据中国法律正式成立的企业，具有签署和履行本合同的资格及履约能力。

2．乙方为签署本合同已经依据适用法律及公司章程之规定完成所有必要的公司内部行为，其有权签署本合同并履行本合同项下的义务。

3．乙方保证向甲方提供本项目服务内容前，已达到提供相应服务的能力，具有相应的资质，包括符合国家、河南省相关标准规范或行业标准规范。

4．乙方有依法缴纳税收和社会保障资金的良好记录；未被“信用中国”网站及“中国政府采购网”网站列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；近三年内（截至签订合同前），在经营活动中没有重大违法违规记录，没有发生过重大质量安全事故。

5．如果乙方的保证或承诺被证明在作出时存在不实或不能兑现，对甲方依本合同享有权利或承担义务造成实质性影响时，甲方有权视影响程度决定是否提前终止本合同，并有权依法进行追责、追偿，本合同各附件也随之自动终止。

6．乙方应当做好网络安全与数据安全工作，遵守国家关于网络安全和数据安全相关的法律法规。

第三条　本项目合同组成

本项目合同由双方协商并载入本合同中的条款、条件，采购文件、投标文件、成交通知书以及以下所提及的附件和有关的补充协议构成。本合同构成文件间有矛盾时，以日期在后的文件为准;双方同意在出现合同理解上的歧义时,能够协商一致的协商解决,否则按照有利于甲方的原则执行。

附件 1：运维服务需求

附件 2：参与运维服务人员名单

附件 3：绩效考核标准

附件 4：廉洁承诺书

附件 5：保密承诺书

第四条　双方的权利和义务

（一）甲方的权利与义务

1.负责在合同生效后向乙方提供关于本项目的相关技术资料。

2.负责提供必要的工作条件、工具和设备。

3.负责做好乙方来现场服务的配合工作和外部协调工作。

4.负责按本合同的约定支付运维费用。

5.甲方指派一名技术人员负责联络和现场协调工作。

6.负责对乙方服务情况的考核、评价等工作。

7.甲方有权对乙方整体运维工作进行监督监控，在服务过程中，如甲方发现乙方的工作质量不符合要求，甲方有权要求乙方进行整改。

8.甲方授权河南省政务大数据中心作为受委托方，负责项目运维服务过程中的技术性管理工作，具体包括：运维需求统筹，技术方案审核，项目安全保障和应急处置，对乙方提供的服务进行考核，对乙方服务质量进行监督，组织参与项目验收。

（二）乙方的权利与义务

1.负责组织技术精湛的现场服务工程师到现场进行服务。

2.乙方来现场技术服务必须遵守甲方的有关合法的规章制度。

3.乙方来现场服务的交通、食宿费用自理。

4.乙方必须对整个运维服务的内容保密，不得将招标文件、合同内容及运维工作中

获取的系统现状及建设情况提供给任何第三方，否则依法追究法律责任。

5.乙方应组建固定的专业基础运行支撑团队报甲方备案，人数不少于____人，实行7×24小时的保障服务，强化运维工作的监督和检查，持续提升运维工作质量。

6.乙方应提供7×24小时响应服务，出现影响系统正常运行的问题应立即响应，简单问题1小时内解决，复杂问题按照绩效考核标准（附件3）中运维故障及信息系统安全事件处置时限要求解决。

7.对甲方相关人员进行业务系统、中间件、数据库等相关技术培训。

8.乙方人员调换及运维服务方案需提交甲方审批。

9.乙方在运维过程中不得擅自留有技术后门以及影响甲方系统安全的其他技术手段，未经甲方书面同意，不得留存或对外提供甲方系统中的数据。

10.针对在运维过程中接触到相关核心数据的人员，每次运维前需制定详细的实施方案，征得甲方书面同意后方可实施。

11.因乙方原因造成合同系统运行出现重大事故、无法访问等问题，造成的一切损失与后果，乙方应承担全部责任。

第五条　本项目服务内容

见附件1：运维服务需求。

第六条　本项目服务期限和地点

（一）服务期限

自合同签订生效之日起至____年__月__日。

（二）服务地点及范围

双方商定，本合同的服务现场地点：郑州。

（三）服务范围：

本项目需要完成以_____/系统/平台为主的软硬件系统的运维，完善运维管理体系，提升系统服务可用性、可靠性和安全性，确保业务的连续性。

（四）服务方式

1.驻现场服务：乙方应当在甲方指定地点安排常驻人员，采取现场服务方式，为甲方提供按合同约定的服务。

2.派现场服务：按甲方要求，乙方到甲方或用户单位，根据甲方要求提供临时技术服务。

3.远程支持服务：通过电话热线、互联网等方式获取远程咨询和技术服务。

4.在本项目服务期间，乙方应当根据服务安排和甲方需求及时调整人员，以适应当前服务需要。合同签订后乙方实际所派项目团队的组成和人员，与《参与运维服务人员名单》保持一致。若因人员离职\辞职\转岗等原因更换团队成员，乙方应当提前报知甲方并经甲方同意。

第七条　合同价格与结算方式

（一）合同价款

1.服务期限内合同总价款为：人民币￥_____元，（大写：_____元整）；含一切税、费。

2.本合同总价包括乙方所提供的所有服务和技术费用，并根据考核约束条件和实际产生费用据实结算，不随通货膨胀的影响而波动。合同总价包括乙方履行本合同义务所发生的一切费用和支出。如发生本合同规定的不可抗力情形，合同总价可经双方友好协商予以调整。

（二）付款方式

本项目合同总价款为人民币小写：￥_____元(含税价),人民币大写：_____元整（含税价）。

1.首期款：签订合同后，乙方书面提交与拟支付金额等额的符合甲方财务管理要求的相应发票后____个工作日内，启动首期款支付流程，支付合同总金额的20%，即人民币大写_____元整（￥_____元）。（如果支付款包含多项费用，应当按大类分别列出支出明细；如果支付的款项需要支付给不同的公司，要按公司分别支付，以下同。）

2.进度款：截至_____年____月____日，结合对前期绩效评估结果，已具备进度款支付条件。甲方在收到乙方书面提交支付申请函及与拟支付金额等额的符合甲方财务管理要求的相应发票后____个工作日内，启动进度款支付流程，支付合同总金额的30%，即人民币大写：_____元整。（￥_____元）。

3.尾款：经甲方确认验收合格后，依据绩效评估结果计算金额扣除已支付金额以及违约金额计算支付，甲方在收到乙方书面提交支付申请函及拟支付金额等额的符合甲方财务管理要求的相应发票后___个工作日内，启动尾款支付流程，即人民币大写_____元整（￥_____元）。

4.乙方在甲方支付合同款项前，应先按各期付款数额在10个工作日内向甲方开具符合国家法律法规和标准的税务发票，之后甲方按程序向乙方进行支付。若乙方未提供

合法有效的发票，甲方有权拒付款项，且不承担违约责任。

（三）乙方账号信息

合同乙方：_____

纳税人识别号：_____

开户名称：_____

开户行：_____

账号：_____

甲方向上述账户汇出款项后，即视为甲方已履行付款义务，在汇款过程中因乙方账户原因（包括但不限于账号被注销、被冻结等）导致其无法收取款项的，由乙方承担相应后果。

第八条　不可抗力和法律变更

（一）本合同中不可抗力指地震、台风、火灾、水灾、战争、疫情以及其他双方共同认同的不能预见、不能避免并不能克服的客观情况。

（二）如发生不可抗力，以致于任何一方因这种事件的发生而无法履行或无法完全履行其义务，一方对另一方因此而造成的损失不承担责任。

（三）遇有上述不可抗力事件的一方，应在可能的时候立即将事件情况通知对方，并在该事件发生后 15 日内向对方提供政府部门开具的有效证明文件，同时提出合同需要延期履行或不能完全履行或不能履行的理由。按照该事件对合同履行的影响程度，由双方友好协商决定继续履行合同或终止合同。

第九条　合同解除/合同终止

（一）合同解除的事由

1.双方在本合同中的声明或保证被证实存在虚假或未兑现，严重影响其履约能力的。

2.出现本合同约定的导致合同终止情形的。

3.发生其他导致本合同无法继续履行情形的。

（二）合同解除程序

1.发出终止意向通知

（1）甲方发出的终止意向通知

下述任一行为发生时，甲方有权立即发出终止意向通知：

①乙方在本合同中的声明或保证被证实存在虚假或未兑现，严重影响其履约能力。

②乙方出现本合同约定的导致合同终止情形的。

③乙方被依法吊销营业执照、责令停业、清算或破产。

④乙方发生累计两（项）或以上严重违约行为。

⑤乙方履行义务不符合约定，经甲方提出后合理期限内仍未改正的。

⑥未经甲方书面同意，乙方将本合同项下属于甲方单方所有的成果作为己用或交付第三人使用的。

⑦第三方指控并经有权机关认定接受乙方提供的服务侵犯了甲方的知识产权和/或其他权利，造成甲方损失的。

（2）乙方发出的终止意向通知

下述任一事件发生时，乙方有权立即发出终止意向通知：

①甲方在本合同中的声明或保证被证实是虚假的或未兑现，使乙方履行本合同的能力受到严重不利影响的。

②甲方无正当理由在逾期 3 个月（自应付日起算）后仍未履行支付义务，但因财政支付管理流程导致的支付延期除外。

2. 法律变更或政府行为

如在本合同生效后，因法律变更及政府行为导致乙方部分或全部不能履行本合同项下主要义务，或在这种情况下已没有继续履行的必要，而这种变化和影响又不以甲方的意志为转移，双方应当尽力就继续履行本合同进行协商，若不能达成一致，则一方可向另一方发出终止意向通知。双方仍协商不成的，本合同自终止意向通知送达对方之日起 10 日届满时终止。

3. 协商一致终止

在本合同履行期间，由各方协商一致可提前终止本合同。费用结算等问题由各方协商一致。

（三）双方协商

1. 终止意向通知发出之后，双方应当在 3 日内协商。

2. 如果双方就将要采取的措施达成一致意见，或者违约行为在指定期限内得到纠正，并获对方确认，终止意向通知即自动失效。

3. 发出终止通知

如终止意向通知发出后，指定期限内违约方仍实施违约行为或违约行为仍未得到纠正，则另一方有权在指定期限届满后合同履约期满前任何时间发出终止本合同的书面通

知，本合同自书面通知送达对方之日起终止。

（四）项目移交

无论因何种原因导致本合同终止，乙方都必须完成甲方合理要求的所有必要工作，将属于甲方的设备、数据、系统、用户文档集、知识产权等资产移交给甲方。甲方可以选择由甲方或甲方指定的第三方接收。甲方设备、数据和系统的风险将在乙方向甲方或其指定的第三方移交并经甲方书面确认之后转移到甲方。在风险转移到甲方之前，甲方的资产发生损坏、缺失、故障的，乙方应当承担相应责任。如因甲方或其指定的第三方原因导致移交出现问题的，乙方不承担责任。

第十条　违约处理

（一）甲乙双方任何一方不履行合同义务或者履行合同义务不符合本合同约定的，均视为违约。守约方可向违约方发出要求其履行合同义务的书面通知，违约方应在通知发出之日起 5 个工作日内采取补救措施；逾期仍未采取措施或采取措施未能实现合同目的的，则守约方有权要求违约方继续履行合同义务并赔偿因此造成的损失。

（二）因甲乙双方任何一方的原因致使另一方遭受第三方追诉的，违约方应赔偿由此给另一方造成的损失（本合同另有约定的除外）。

（三）合同履行过程中，发生下列情形之一的，乙方按照合同总金额的比例支付相应的违约金；给甲方造成损失的，赔偿损失。

1.信息系统出现故障或安全事件，乙方未能按绩效考核标准（附件 1-3），或处理时限严重超期，按合同总金额万分之五/次扣除执行；

2.乙方违反信息保密安全义务，出现泄密或信息泄露的情况，按合同总金额百分之三十/次扣款执行。

（四）乙方原因导致出现重大及以上安全事件，或因乙方的其他违约行为，给甲方造成重大损失或重大影响的，甲方有权解除合同，并按有关法律追究责任，请求赔偿损失。

（五）乙方运维达不到法定或约定标准或质量的，甲方有权委托第三方代为运维，费用由乙方承担。甲方可从应向乙方支付的费用中直接扣除。

（六）甲方未按照本合同约定付款方式付款，甲方支付应付金额的万分之三的违约金。

（七）因乙方违反《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》等法律法规和相关规定，造成系统出现安全问

题，造成一般后果的，甲方有权每次扣除合同金额的1%；造成严重后果的，每次扣除合同金额的10%；上述扣除金额合计超过合同总金额30%，甲方有权解除合同并依法追究乙方责任。

第十一条　争议解决

（一）因履行合同所发生的一切争议，双方应当友好协商解决，协商不成的，双方均同意向甲方所在地人民法院提起诉讼。

（二）在诉讼进行过程中，双方应当继续履行本合同未涉诉的其他部分（合同被解除或终止的除外）。

（三）双方对于合同履行期间难以确定过错归属的，可以向双方认可的第三方机构申请鉴定，确认责任。鉴定费用由主张对方存在过错的一方先行垫付，最终由鉴定存在过错的一方承担。

第十二条　其他约定

（一）本合同未尽事宜，甲乙双方可签订补充协议，补充协议与本合同具有同等法律效力。

（二）招标文件、投标文件、在本合同实施过程中双方共同签署的补充协议与修正文件（若有）均为本合同的组成部分。

（三）乙方应当做好安全保密工作，签订保密协议，并组织开展安全教育培训。

（四）合同变更与修订

除另有约定，本合同任何修改、补充或变更必须经双方协商一致，并书面签订补充协议。如果本合同的任何条款不合法、无效或不能执行，则：

1.并不影响其他条款的效力和执行；

2.双方应当商定对不合法、无效或不能执行的条款进行修改，使之合法、有效并可执行；修改或更改应当尽可能平衡双方之间的利益。

（五）合同适用法律

本合同的成立、有效性、解释、履行、签署、修订、终止和解除以及争议的解决适用中华人民共和国法律法规及相关规定。

（六）通知

1.本合同约定的联系地址、联系方式为双方唯一联系地址、联系方式。甲、乙双方因履行本合同而需由一方发给对方的任何通知应当以书面方式发出。该通知可以专人送达、传真、电子邮件、特快专递或挂号方式送达的方式发出。如联系地址或联系方式有

变动的，应当至少提前 15 日内书面通知对方。双方发生争议后，甚至进入诉讼程序，该联系地址、联系方式仍有效。

2. 上述通知、要求或信息，以专人送达的，以受送达人在送达回执上的签收时间为送达日期；以传真方式送达的，以发送之日为送达日期；以电子邮件方式送达的，以到达受送达人特定系统的日期为送达日期；以特快专递或挂号方式送达的，以受送达人在相应邮寄凭证上签收之日为送达日期。上述联系地址或联系方式发生变动且未及时书面通知另一方的，另一方按原地址邮寄相关材料即视为已履行送达义务。

（七）合同生效条件

本合同经双方法定代表人（负责人）或授权代表签字且盖章后生效。

（八）合同份数

本合同一式肆份，甲方执贰份，乙方执贰份，具有同等法律效力。

（以下无正文，仅为签章页）

甲方（盖章）：_____

_____

法定代表人或授权代表

（签字）：_____

统一社会信用代码：_____

联系人：_____

联系电话：_____

地址：_____

2026 年　月　日

乙方（盖章）：_____

_____

法定代表人或授权代表

（签字）：_____

统一社会信用代码:_____

开户银行及账号：_____

联系人：

联系电话：

地址：

2026 年　月　日

附件 1-1

运维服务需求

河南省行政审批和政务信息管理局 2026 年度局属政务信息系统运维项目招标文件“第五章采购需求”。

附件 1-2

参与运维服务人员名单

序号	姓名	性别	职称	专业	电话	对口负责系统
1						
2						
3						
4						
5						
6						
...						
...						
...						

附件 1-3

A 包、B 包、C 包绩效考核标准

考核时间：　　年　月　日——　　年　月　日					
考核主项	**考核细项**	**考核内容**	**满分**	**考核扣分项**	**考核扣分**
基础运行支撑服务(100分)	服务质量	1.按时高质量完成基础环境软件运维报告、业务系统运维、安全运维报告编制。	30	每缺1份报告扣1分；	
		2.按运维需求要求及时响应服务。		发现一次服务响应不及时扣2分，无响应扣5分，扣完为止。	
		3.按时完成系统全面巡检工作。		未按时完成系统巡检，每次扣1分，未巡检每次扣2分。	
	运维故障及信息系统安全事件处置	网络安全事件处置时限要求： 特别重大网络安全事件（Ⅰ级）： ≤20分钟响应，12小时处置 重大网络安全事件（Ⅱ级）： ≤30分钟响应，24小时处置 较大网络安全事件（Ⅲ级）： ≤60分钟响应，36小时处置 一般网络安全事件（Ⅳ级）： ≤90分钟响应，48小时处置。	20	未按相关规范流程和时限处置一级、二级运维故障及信息系统安全事件，每发生1次扣10分； 未按相关规范流程和时限处置三级、四级运维故障及信息系统安全事件，每发生1次扣5分。	
	安全	1.包括网络和信息安全责任承诺书的签订和与系统相关的安全保密工作。	10	未按规定执行，每少1项扣5分。	
		2.制定重保方案，完成重保支撑工作。	10	未按规定制定重保方案，每次扣5分；未按重保方案实施重保，方案中每有一项未	

	保密			实施扣2分。	
		3.安全漏洞修复和处置时间要求：高风险3天；中风险7天。	10	未按规定时间完成安全漏洞修复和处置，高风险每次扣0.2分，中风险每次扣0.1分。	
	应急响应	1.制定应急预案，完成应急响应和应急演练准备。 2.发生紧急情况时组织人员完成应急响应。	15	未制定应急预案扣5分；发生紧急情况时未提供应急支持服务每次扣5分；每年实施2次应急演练，每缺一次扣2.5分。	
	人员保障	满足人员岗位配置要求。	5	每1人不满足扣0.5分，扣完为止。	
否决项	重大及以上安全事件	出现泄密、数据泄露、服务中断等行为导致国家、省级有关部门督导的情况。	/	出现一次重大及以上事件，甲方有权终止合同。	
总分（100分）			100		

服务款项结算标准

序号	评价分数范围	评价等级	支付比例
1	90 分≤评价≤100 分	优秀	100%
2	75 分≤评价<90 分	良	90%
3	60 分≤评价<75 分	中等	70%
4	评价低于 60 分	不合格	50%

备注：

1．服务结算标准是依据服务质量评价结果确定的服务费的支付比例。

2．上述结算标准仅作为甲方对乙方的服务质量评价结算标准，不作为验收条件。

3．计算公式：服务金额=合同总金额*评价分数对应的支付比例。

D包绩效考核标准

考核时间：　　年　月　日——　　年　月　日					
考核主项	**考核细项**	**考核内容**	**满分**	**考核扣分项**	**考核扣分**
基础运行支撑服务(100分)	服务质量	1.按时保质保量完成基础环境、软件运维报告、安全服务报告。	30	每缺1份报告扣1分；	
		2.按甲方要求及时响应服务。		发现一次服务响应不及时扣2分，无响应扣5分，扣完为止。	
		3.按时完成系统全面巡检工作。		未按时完成系统巡检，每次扣1分，未巡检每次扣2分。	
	运维故障及信息系统安全事件处置	网络安全事件处置时限要求： 特别重大网络安全事件（Ⅰ级）： ≤20分钟响应，12小时处置 重大网络安全事件（Ⅱ级）： ≤30分钟响应，24小时处置 较大网络安全事件（Ⅲ级）： ≤60分钟响应，36小时处置 一般网络安全事件（Ⅳ级）： ≤90分钟响应，48小时处置。 运维故障处置时限要求： 一级故障:≤3分钟响应,0.5小时处置 二级故障:≤5分钟响应，1小时处置 三级故障:≤10分钟响应，2小时处置 四级故障:≤15分钟响应，4小时处置	20	未按相关规范流程和时限处置一级、二级运维故障及信息系统安全事件,每发生1次扣10分； 未按相关规范流程和时限处置三级、四级运维故障及信息系统安全事件，每发生1次扣5分。	
		1.包括网络和信息安全责任承诺书的签订和与系统相关的安全保密工	10	未按规定执行，每少1项扣5分。	

		作。			
	安全保密	2.制定重保方案，完成重保支撑 工作。	10	未按规定制定重保方案，每次扣5分；未按重保方案实施重保，方案中每有一项未实施扣2分。	
		3.安全漏洞修复和处置时间要求：高风险7天；中风险14天。	10	未按规定时间完成安全漏洞修复和处置，高风险每次扣0.2分，中风险每次扣0.1分。	
	应急响应	1.制定应急预案，完成应急响应和应急演练准备。 2.发生紧急情况时组织人员完成应急响应。	15	未制定应急预案扣5分；发生紧急情况时未提供应急支持服务每次扣5分；每年实施2次应急演练，每缺一次扣2.5分。	
	人员保障	满足人员岗位配置要求。	5	每1人不满足扣0.5分，扣完为止。	
否决项	重大以及上安全事件	出现泄密、数据泄露、服务中断等行为导致国家、省级有关部门督导的情况。	/	出现一次重大及以上安全事件，甲方有权终止合同。	
总分（100分）			100		

服务款项结算标准

序号	评价分数范围	评价等级	支付比例
1	90 分≤评价≤100 分	优秀	100%
2	75 分≤评价<90 分	良	90%
3	60 分≤评价<75 分	中等	70%

4	评价低于 60 分	不合格	50%

备注：

1．服务结算标准是依据服务质量评价结果确定的服务费的支付比例。

2．上述结算标准仅作为甲方对乙方的服务质量评价结算标准，不作为验收条件。

3．计算公式：服务金额=合同总金额*评价分数对应的支付比例。

附件 1-4

廉洁承诺书

为加强商务活动中的廉政建设，防止发生各种谋取不正当利益的违法违纪行为、规范合同双方的各项活动，保障顺畅、公平的商业秩序，保护当事人的合法权益，根据《中华人民共和国民法典》等相关法律，我司承诺以下廉政责任：

一、我司承诺在与甲方的商务往来活动中遵循自愿、公平、等价有偿、诚实信用原则，并保证在合同订立、履行过程中以及事前事后保持公开、公平、公正、诚信、透明的原则，不会为获取不正当的利益，损害国家、集体和甲方利益。

二、我司保证我司以及我司工作人员与甲方保持正常的业务交往，按照有关法律法规的规定和程序开展业务活动，并遵守以下规定：

（一）不以任何理由向甲方工作人员提供或赠送礼金、有价证券、贵重物品及回扣、好处费、感谢费等。

（二）不以任何理由为甲方工作人员报销应由甲方工作人员个人支付的费用。

（三）不接受或暗示为甲方工作人员在装修住房、婚丧嫁娶、配偶子女的工作安排以及出国（境）、旅游等方面提供便利。

（四）不为甲方工作人员提供通信工具、交通工具和高档办公用品等物资。

（五）不以任何理由为甲方工作人员组织有可能影响廉洁、公正的宴请、健身、娱乐活动。

（六）不许诺事后给予甲方工作人员利益。

（七）不以其他手段为甲方工作人员提供其他不正当利益。

（八）上述条款中所称不正当利益包括但不限于金钱和实物。如回扣、佣金、股份、股东资格、债券、促销费、赞助费、广告宣传费、劳务费、红包、礼金、含有金额的会员卡、代币卡（券）、旅游费用、就业机会、项目机会、各种高档生活用品、奢侈消费品、工艺品、收藏品、房屋、车辆、减免债务、提供担保、免费娱乐、旅游、考察、提供房屋装修、借贷款项、借用物品、特殊待遇等财产性或者非财产性利益等。

三、我司同意，如违反以上约定，甲方有权终止合同，相关的责任由我司承担；涉嫌犯罪的，甲方有权移交司法机关，并追究刑事责任。若因此给甲方造成经济损失的，我司同意按有关规定予以赔偿。

承诺方（盖章）：_____

签字日期：_____年____月____日

附件 1-5

保密承诺书

为明确乙方所应履行的网络信息安全责任，确保网络信息安全，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《关键信息基础设施安全保护条例》、《网络安全审查办法》等相关法律、法规的规定，制定本责任书，具体内容如下：

一、乙方严格遵守国家有关法律、法规，严格执行网络安全、数据安全、信息安全管理规定。

二、依照法律、行政法规的规定和国家标准的强制性要求，乙方采取必要措施，保障服务范围内信息系统的安全、稳定运行，快速应对网络安全事件，不得在提供或研发的软件、服务中设置恶意程序或后门。

三、乙方应强化技术防范，严格安全管理，切实提高防攻击、防篡改、防病毒、防瘫痪、防窃密能力。

四、针对乙方在甲方的授权下获得的或获知的涉及甲方或甲方客户的各类保密信息，包括但不限于甲方的商务资料、技术信息资料、工程建设资料、网络技术资料、财务资料、账务资料、客户资料、企业各类信息、商业秘密、其他保密信息等，上述保密信息的储存方式包括但不限于书面文件、电子文档、数据格式、资料图像、音像资料、以及物件等信息载体。乙方承诺仅为项目合同目的在双方合作合同履行过程中使用涉及甲方所有的保密信息，不为任何其他目的使用保密信息。

五、未经甲方的事先书面批准，乙方不得以任何形式或任何方式将上述保密信息和/或其中的任何部分，披露或透露给任何第三方。乙方有义务妥善保管保密信息，不得复制、泄漏或遗失。未经甲方的同意乙方不得向其职员透露上述保密信息/或其中的任何部分。如经得甲方同意，乙方能够知悉上述保密信息的职员应是乙方参与项目合同的相关人员。

六、未经甲方的事先书面批准，乙方不利用取得的账号权限，非法窃取、泄露，或违规拷贝、下载、存储、使用甲方或甲方客户的各类保密信息；

七、乙方的职员违背保密承诺，未按照本责任书的规定使用保密信息或向第三方披露保密信息，或依据该等保密信息向第三方做出任何建议，都被视为乙方违反本责任

书。乙方的职员违背保密承诺，未按照本责任书的规定使用保密信息或向第三方披露保密信息，或依据该等保密信息向第三方做出任何建议，都被视为乙方违反本责任书。因乙方员工所造成的违约责任，由乙方承担。

八、如果因乙方的违约行为造成甲方的损失，乙方应当赔偿甲方全部损失，包括甲方因乙方的违约行为所受到的实际经济损失，甲方因调查乙方的违约行为而支付的合理费用，以及争取补救措施所引起的所有费用和损失。

九、因乙方的违约行为侵犯了甲方的商业秘密权利或合法权益的，甲方可以选择根据本责任书要求乙方承担违约责任，或者根据国家有关法律、法规要求乙方承担侵权责任，并追究其刑事责任。

十、本责任书未尽事宜按照国家有关法律规定执行。

承诺方（盖章）：_____

日期：_____年____月____日

合同登记编号：

局属信息系统网络安全等级保护测评项目合同

（E 包）

项目名称：_____

委托方（甲方）：_____

受托方（乙方）_____

签订地点：河南郑州

局属信息系统网络安全等级保护测评项目

服务合同

甲方：

乙方：

按照《中华人民共和国民法典》《中华人民共和国政府采购法》，经_____（以下简称甲方）和中标单位_____（以下简称乙方）在友好协商、平等互惠的基础上，就甲方委托乙方承担局属信息系统网络安全等级保护测评项目的有关事项达成一致意见，签订本合同，经双方确认，一致同意以下条款，以资共同遵守：

第一条 术语和定义

在本合同中，下列术语及定义，除上下文另有约定外，应具有本条所赋予的含义。

1.1 “一方”：指甲方或乙方中的任何一方。

1.2 “双方”：指甲方和乙方。

1.3 “合同”：指双方就本项目达成并签署的协议，包括所有的附件，以及下面指出的构成合同的所有文件。双方同意下列文件作为本合同不可分割的组成部分：

1.3.1 本合同正文；

1.3.2 本合同附件；

1.3.3 在本合同履行过程中双方共同签署的补充与修正文件。

1.4 “合同总价”：指根据合同规定，在乙方全面正确地履行合同义务时甲方应支付给乙方的总金额。包括完成本项目所需的服务费、人工费、交通费、食宿费、工具购置费、测试费、税费、验收费等完成本项目全部内容所需的所有费用。

1.5 “工作日”：即标准工作日，指国家所规定的节假日之外的所有工作日，未指明为工作日的日期指自然顺延的日期。

1.6 “信息系统”：是由计算机硬件、网络和通信设备、计算机软件、信息资源、信息用户和规章制度组成的以处理信息流为目的的人机一体化系统。

1.7 “秘密”：指甲方所拥有的，不为公众所知的管理信息、方式方法、用户名单、数据、信息、技术诀窍、源代码、计算机文档等，或由双方在履行本合同过程中明确指明为秘密的、法律所认可的任何信息。

1.8 “重大故障”：指乙方在测评服务过程中，由于失责或操作不当导致应用系统

整体运行中断无法正常使用并且不能够在4小时以内解决的故障问题。

1.9 “附件”：指与本合同的订立、履行有关的，经双方书面认可的，对本合同约定的内容进行细化、补充、修改、变更的文件、图纸、音像制品等资料。

第二条 本项目合同组成

本项目合同由双方协商并载入本合同中的条款、条件，磋商文件、应答文件、成交通知书以及所提及的附件和有关的补充协议构成。本合同构成文件间有矛盾时，以日期在后的文件为准；双方同意在出现合同理解上的歧义时，按照有利于甲方的原则执行。

第三条 服务期间和服务地点

3.1 技术服务期限

3.1.1 合同签订生效后至____年____月____日。

3.1.2 具备测评条件之日起_____个工作日内完成现场测评。

3.2 技术服务地点

河南省郑州市或甲方指定的其他地点。

3.3 服务方式

3.3.1 以文字报告的方式提供服务。

3.3.2 安排相关技术人员提供现场测评服务。

第四条 服务内容和范围

4.1 甲方委托乙方提供本项服务工作，乙方承诺为甲方以下信息系统提供网络安全等级保护测评：

序号	局属信息系统分项名称	等保等级
1	河南省省级一体化政务服务平台	三级
2	河南省政务服务移动端“豫事办”(一期)	三级
3	河南省“豫正通”	三级
4	河南省电子政务外网管理中心（一期）	三级
5	河南省“互联网+监管”系统（一期）	三级
6	河南省一体化协同办公平台	三级

7	河南省大数据中心(一期)	三级

4.1.1 按照网络安全等级保护最新测评相关要求，对甲方的被测系统进行测评。

4.1.2 汇总、整理和分析测评结果，提出相应整改建议，协助甲方开展系统安全整改工作。

4.1.3 按照甲方要求，协助完成系统备案等工作。

4.1.4 按照甲方要求，并结合实际工作需要，必要时调整被测系统定级级别，以最终实际定级、备案级别为准。

4.2 服务阶段。

4.2.1 分为测评准备阶段、方案编制阶段、现场测评阶段（含复测）、分析与报告编制阶段。

4.2.2 各阶段需交付的测评过程文档按照项目招标文件要求提供。

4.3 服务机构、职责与人员配备安排。

4.3.1 乙方按照服务内容和目标要求成立等级保护测评服务小组。服务小组在项目经理领导下，按照项目要求和目标任务确定工作职责，于项目启动后 1 日内建立健全各项规章制度。

4.3.2 乙方根据项目要求和甲方需要配备有关专业人员，提供____名项目经理，具有信息安全等级测评师证书（高级），并具有信息系统安全等级测评相关资质或证书。提供不少于_____名测评人员,具有 3 年以上从事信息系统安全等级测评服务工作经验，并具有信息系统安全等级测评相关资质或证书。

4.4 售后服务要求

4.4.1 乙方提供 1 年免费售后服务技术支持，提供 7×24 小时远程服务，必要时 2 小时内到达现场提供紧急情况的应急支持服务，确保 8 小时内解决问题。

4.4.2 服务期内，乙方按照甲方需求提供巡检服务，并协助整改服务、漏洞扫描服务等。

4.4.3 服务期内，乙方提供不少于 2 次网络安全培训服务，培训内容包含但不限于安全意识教育、等级保护、安全知识等。

第五条 服务要求

5.1 乙方应严格建立质量保证体系，制定项目建设的质量控制方案和实施措施，并督促完成各环节质量控制内容和目标；保证项目各个阶段满足甲方对质量的要求。

5.2 乙方应根据项目的工作计划，对阶段性项目工作成果进行审核，并向甲方提交里程碑式工作成果。通过保证各阶段性成果的质量，最终保证整个项目的质量。

5.3 所有提交给甲方的技术报告及相关的资料的最后文本，包括为履行技术服务范围所编制的图纸、计划和证明资料等，都属于甲方的财产，乙方在提交给甲方之前应将上述资料进行整理归类和编制索引。

5.4 未经甲方的书面同意，乙方不得将上述资料用于本服务项目之外的任何项目。

第六条 服务标准

按照《信息安全等级保护管理办法》（公通字〔2007〕43 号）、《信息系统安全等级保护实施指南》（信安字〔2007〕10 号）和《信息安全等级保护安全建设 整改工作指导意见》（公信安〔2007〕1429 号）（含附件）等公安部信息安全等级保护系列文件要求，对系统清单中的局属信息系统开展网络安全等级保护测评，具体信息安全技术标准以文件相应部分提及的为准，国家标准和国际标准不一致的地方则参照国家标准。

6.1 需遵循的政策法规

（1）《中华人民共和国网络安全法》（2017年6月1日正式实施）

（2）《中华人民共和国保守国家秘密法》（1988年9月5日中华人民共和国主席令第6号公布）

（3）《中华人民共和国保守国家秘密法实施办法》（国家保密局文件国保发〔1990〕1号）

（4）《中华人民共和国国家安全法》（主席令68号，1993年2月22日第七届全国人民代表大会常务委员会第三十次会议通过）

（5）《中华人民共和国计算机信息系统安全保护条例》（国务院令147号）

（6）《计算机信息系统保密管理暂行规定》(国家保密局文件国保发〔1998〕1号）

（7）《计算机信息系统国际联网保密管理规定》(国家保密局文件国保发〔1999〕1号）

（8）《中华人民共和国计算机信息网络国际联网管理暂行规定》（国务院令195号）

（9）《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》（1997年12月8日国务院信息化工作领导小组审定）

（10）《计算机病毒防治管理办法》（2000年4月26日中华人民共和国公安部第51号令）

（11）《计算机信息网络国际联网安全保护管理办法》（1997年12月11日国务院批准，1997年12月30日公安部发布）

（12）《计算机信息系统安全专用产品分类原则》（1997年4月公安部发布）

（13）《互联网电子公告服务管理规定》（信息产业部2000年10月8日第4次部务会议通过）

（14）《计算机信息系统安全等级保护划分准则》（GB/T17859-1999）

（15）《计算机信息系统安全等级保护网络技术要求》（GA/T387-2002）

（16）《计算机信息系统安全等级保护操作系统技术要求》（GA/T388-2002）

（17）《计算机信息系统安全等级保护数据库管理系统技术要求》（GA/T389-2002）

（18）《计算机信息系统安全保护等级划分准则》（1999年9月国家技术监督局发布）

（19）《计算机信息系统安全等级保护通用技术要求》（GA/T390-2002）

（20）《计算机信息系统安全等级保护管理要求》（GA/T391-2002）

（21）《计算机机房场地安全要求》（GB9361-88）投标人必须遵循但不限于以上法律法规。

6.2 行业规范

(1)《信息安全等级保护管理办法》(公通字〔2007〕43号)

(2)《信息安全技术 网络安全等级保护实施指南》(GB/T 25058-2019)

(3)《信息安全等级保护安全建设整改工作指导意见》(公信安〔2009〕1429号)(含附件)

(4)《信息安全技术 网络安全等级保护定级指南》（GA/T 1389-2017）

(5)《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

(6)《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

(7)《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）

第七条 双方的权利与义务

7.1 甲方的权利和义务

7.1.1 甲方应当依据本合同的约定，向乙方支付测评服务价款。

7.1.2 甲方为乙方提供本合同项下所需要的资源，包括访问测评范围内网络设备和主机设备的权限及其他相关资料。

7.1.3 甲方确保乙方实施本合同项下的服务时，对于设备的使用、信息的获取和更改，不会违反任何保密或协议责任，不会侵犯第三方的权利。

7.1.4 甲方有权在乙方履行合同过程中出现损害或可能损害国家利益、公共利益、公共安全情形时变更、中止或者终止本合同。

7.1.5 甲方授权河南省政务大数据中心作受委托方，负责项目运维服务过程中的技术性管理工作，具体包括：项目需求统筹，技术方案审核，项目安全保障和应急处置，对乙方提供的服务进行考核，对乙方服务质量进行监督，组织参与项目验收。

7.2 乙方的权利和义务

7.2.1 乙方应当按照甲方的要求，制定适用于本合同服务范围的内部质量和风险控制制度及措施，确保完成本项目的测评服务。

7.2.2 乙方人员在项目执行期间应保持相对稳定，以保证项目的顺利实施。乙方人员的变更需提前 3 日向甲方提出书面申请，并保证接替人员能够胜任此项测评工作，经甲方书面同意后方可变更，变更时做好该项目的技术及文档交接。参与项目的所有人员都应当受本合同各条款的约束。

7.2.3 乙方须确保乙方及项目组人员遵守附件 3《保密承诺书》的各项内容。

7.2.4 乙方在按合同要求实施测评的过程中，应当及时向甲方通报在信息系统中发现的安全问题，并协助甲方尽可能地弥补缺陷。

7.2.5 乙方应当接受并配合甲方组织的对本合同履行情况的监督与检查，对于甲方指出的问题，应及时作出合理解释或予以纠正。

7.2.6 乙方应当根据甲方要求，接受和配合甲方或甲方委托机构进行的与本合同相关的审计。

7.2.7 乙方在项目实施过程中出现资源、进度、质量协调控制不力的情况，甲方有权要求更换相关项目人员，乙方必须予以配合，并确保不影响项目的进度和质量。

7.2.8 乙方应当根据服务的内容和进度安排，按时提交阶段性技术报告及有关资料。

7.2.9 乙方在实施关键测评项时（如漏洞扫描或工具测试等），要与甲方充分沟通该关键测评项实施的细节与步骤，得到甲方许可后，再开展该测评，以该测评项对甲方的信息系统影响最小化为目标。

7.2.10 项目交付后，乙方应当无条件返还甲方提供的文件、资料，同时乙方应当自留一份完整的项目档案按保密信息标准予以妥善保存，以便质保工作的顺利开展，但不得用于第三方和其他项目。

第八条 项目验收

8.1 乙方服务完成后，向甲方提交验收申请，由甲方组织项目的验收工作，乙方在合同期满前提交以下项目文档：

8.1.1 提交被测系统的《网络安全等级保护测评方案》；

8.1.2 提交被测系统的《网络安全等级保护漏洞测试报告》；

8.1.3 提交被测系统的《网络安全等级保护测评报告》；

8.1.4 根据测评中反映出的安全问题，汇总、整理、分析测评结果，按照适度有效的原则，向甲方提交《信息系统安全等级保护整改方案》；

8.2 甲方收到以上文档后，组织人员开展验收。

8.3 验收完毕后，乙方应持续协助甲方开展整改工作，对整改后的成效按验收标准进行评审，重新出具测评报告。

第九条 合同价款、支付方式及履约保证

9.1 本项目合同总价款为人民币小写：￥_____元，（含税价），人民币大写_____元整（含税价）。

9.2 首期款：签订合同后，乙方书面提交与拟支付金额等额的符合甲方财务管理要求的相应发票后____个工作日内，启动首期款支付流程，支付合同总金额的30%，即人民币大写_____元整（￥_____元）。（如果支付款包含多项费用，应当按大类分别列出支出明细；如果支付的款项需要支付给不同的公司，要按公司分别支付，以下同。）

9.3 尾款：经甲方确认验收合格后，依据绩效评估结果计算金额扣除已支付金额以及违约金额计算支付，甲方在收到乙方书面提交支付申请函及拟支付金额等额的符合甲方财务管理要求的相应发票后__个工作日内，启动尾款支付流程，即人民币大写_____元整（￥_____元）。

9.4 乙方在甲方支付合同款项前，应先按各期付款数额在10个工作日内向甲方开具符合国家法律法规和标准的税务发票，之后甲方按程序向乙方进行支付。若乙方未提供合法有效的发票，甲方有权拒付款项，且不承担违约责任。

第十条 合同变更

10.1 如本合同在履行过程中有任何变更、补充或修改，都必须经甲乙双方协商同意，必要时依据重要程度由双方法定代表人或授权代表另行签订书面协议。

10.2 甲方提出变更要求

10.2.1 如甲方要求变更项目服务内容，应当以书面形式将相关要求提交给乙方。乙方应当在7个工作日内，对该变更后在项目交付日期、工作量、影响范围等方面做出评估，并书面回复甲方。

10.2.2 甲方在收到乙方回复后，应当在7个工作日内，以书面方式通知乙方，对是否接受进行回复。因甲方提出的变更导致工作量增加的，如果增加的工作量不超过总量的20%，则合同总价不作调增；因甲方提出的变更导致工作量减少的，如果减少工作量不超过总量的20%（含），则合同总价不作调减。如果增加工作量超过总量的20%，甲方将视增加的服务为新项目，另行立项。如果减少工作量超过总量的20%，经双方共同协商后，签订补充协议，按比例调整合同总价。

10.2.3 合同履行期间甲方因业务职能或重大政策发生变更或因其他原因导致合同无法继续履行时，甲方有权解除本合同，且不承担任何违约责任。合同未履行部分的费用不再支付，已支付部分按未实施的服务部分比例或剩余服务时间的比例进行返还，未支付部分按已实施的服务部分时长与全年时长比例进行支付。

10.3 乙方提出变更建议

10.3.1 如乙方要求变更项目服务内容，乙方应当对该变更后在项目交付日期、工作量、影响范围等方面做出评估，并以书面形式提交给甲方。

10.3.2 甲方在收到乙方的变更建议后，应当在7个工作日内，以书面方式通知乙方是否接受乙方的变更建议。如甲方接受乙方的变更建议，因乙方提出的变更导致工作量增加的，则合同总价不作调增；因乙方提出的变更导致工作量减少的，如果减少工作量不超过总量的20%（含），则合同总价不作调减。如果减少工作量超过总量的20%，则经双方共同协商后，签订补充协议，按比例调整合同总价。

第十一条 知识产权

11.1 乙方在履行和完成本合同项下工作过程中准备及形成的一切资料，包括但不限于文件、计算方法、图表、报告、数据、模型和样品，以及其中含有的所有发明为甲方所有，甲方有权使用上述资料以履行本项目合同或用于其他目的。该资料应与本项目合同项下其他资料一起，按要求在本项目合同结束或终止的时候，交还给甲方。

11.2 本项目所形成的产品其知识产权归甲方所有，乙方非经甲方书面同意，不得以任何方式向第三方披露或转让。除本项目测评需要外，乙方不得以任何方式在任何情形下利用。

11.3 涉及乙方的测试流程、测试方法、分析方法、方案模板、报告模板等相近知

识产权内容归乙方所有。

第十二条 保密

乙方须与甲方签订保密承诺书作为合同附件，见附件 3。

第十三条 违约责任及损失赔偿

13.1 如果乙方在工作中发生重大及以上安全事件，包括但不限于由于乙方故意或过失等原因造成甲方系统出现重大网络中断、数据丢失、系统瘫痪或者出现反动言论等情况或者因测评不符合合同要求，严重影响到甲方正常的业务工作，甲方有权决定是否解除合同，乙方须承担由此给甲方带来的一切损失。

13.2 乙方违反合同约定的保密义务，乙方应当支付合同总价 1%的违约金。如实际损失超过违约金的，甲方有权要求对方赔偿超过部分。

13.3 任何一方违反合同约定的知识产权保护条款，除立即停止违约行为外，还应当支付合同价款的 1%作为违约金。

13.4 乙方工作人员未经甲方授权，擅自篡改甲方业务数据，或利用甲方现有业务信息系统、网络平台或者冒用甲方身份获取非法利益，造成甲方或任何第三方损失的，由乙方承担法律责任并负责赔偿全部损失，同时乙方须向甲方支付本合同总价款 1%的违约金。

13.5 因乙方原因造成严重超期、拖延而不能按时交付，自交付日期起，每超期一周乙方应当支付合同总价 1%的违约金。

13.6 如乙方工作人员擅自承担或参与涉及甲方职能的行政业务工作，对甲方造成不良影响的，乙方应立即停止其行为并采取发布声明等措施消除影响，同时甲方保留追究乙方法律责任的权利。

13.7 如乙方发生违约事件，甲方要求乙方支付违约金或赔偿款时，应当以书面方式通知乙方，内容包括违约事件、违约金、支付时间和方式等。乙方在收到上述通知后，应当于 7 日内答复甲方，并支付违约金或赔偿金。逾期未支付的，甲方有权在合同款项中予以扣除。

13.8 服务期限内，如乙方发生违约事件累计超过三次，甲方有权单方终止合同，并将乙方列入不良行为记录，甲方有权限制乙方参与甲方此后的测评服务项目。

第十四条 不可抗力

14.1 本合同中不可抗力系指甲乙双方在缔结合同时所不能预见的、并且它的发生及其后果是无法避免和无法克服的客观情况。

14.2 由于不可抗力致使合同无法履行的，受不可抗力影响一方应立即将不能履行本合同的事实书面通知对方，并协助对方最大可能减少损失，在不可抗力发生之日起 7 日内提供有关政府部门或公证机关出具的证明文件。

14.3 本合同在不可抗力影响范围及其持续期间内将中止履行，本合同执行时间可根据中止的时间相应顺延，双方无需承担违约责任。不可抗力事件消除后，双方应当就合同的履行及后续问题进行协商。

第十五条 合同转让及终止

15.1 合同转让：非经双方书面同意，任何一方无权转让本合同及该合同约定的全部或部分权利、义务。非经对方同意擅自转让的，对方有权解除合同，并要求擅自转让方承担全部赔偿责任。

15.2 合同终止

15.2.1 合同自然终止：甲乙双方全部履行合同约定的义务后，本合同自然终止。

15.2.2 违约合同终止：若合同一方有足够证据证明合同另一方未在规定时间履行本合同项下规定义务，可向对方提出书面违约通知，提出终止部分或全部合同，合同中未终止的部分应继续履行。

15.2.3 无能力履行合同终止：如有充分证据证明乙方无清偿能力或无继续履行合同的能力，甲方可以在任何时候以书面形式通知对方，提出终止合同而不给对方补偿，或要求资产保全防止损失扩大。

15.3 双方协商一致可以终止合同。

第十六条 适用法律及争议解决

16.1 本合同按中华人民共和国法律解释。

16.2 甲、乙双方在合同履行过程中发生的一切争议，均应通过双方友好协商解决；协商不成的，任何一方均可向甲方住所地人民法院提起诉讼。

16.3 在诉讼期间，除正在进行诉讼的部分外，本合同的其他部分应当继续执行。

第十七条 合同的生效

17.1 本合同经双方盖章以及法定代表人或授权代表签字后生效。

17.2 本合同一经签署，未经双方书面同意，任何一方不得随意更改。

17.3 本合同一式肆份，甲乙双方各执贰份，具有同等法律效力。

第十八条 其他

18.1 如一方改变通讯地址及其他信息，应当在变更后 7 日内以书面方式通知另一

方，否则，由此而造成的损失，由信息发生变更的一方承担。

18.2 本合同未尽事宜，双方可以另行协商签订补充协议，补充协议经双方盖章以及法定代表人或授权代表签字后与本合同具有同等效力。

（以下无正文，仅为签章页）

甲方（盖章）：_____

法定代表人或授权代表（签字）：_____

统一社会信用代码：_____

联系人：_____

联系电话：_____

地址：_____

2026 年　月　日

乙方（盖章）：_____

法定代表人或授权代表（签字）：

统一社会信用代码:_____

开户银行及账号：_____

联系人：_____

联系电话：_____

地址：_____

2026 年　月　日

附件 1-1

参与项目人员名单

序号	姓名	职务	执业资格	从事相近工作年限	电话（手机）
1					
2					
3					
4					
5					
6					
7					
8					

附件 1-2

绩效考核标准

序号	评价类别	评价指标	评分内容	分值
1	服务评价基本项	服务规范性	(1)按照国家和河南省有关验收规定和要求提供对应的服务； （2）等保测评服务符合国家标准的相关规定。	10 分
2		沟通协调	（1）建立顺畅高效的沟通平台或沟通机制，开展与各干系人的沟通工作，保障各类信息、问题、解决方法在各干系人和相关方的沟通； （2）能与甲方进行及时有效的沟通，保障服务提供方的利益，创造适宜的沟通平台，保障信息及时、完整地传达到相关人员或单位。	10 分
3		计划管理	（1）准确、科学、详实地编制项目整体等保测评计划、等保测评方案等，具有较强的计划管理能力，在等保测评执行中能进行及时改进和优化等保测评方法。 （2）完成首轮测评后，定期追踪问题整改进度，推进项目测评进度。	10 分
4		等保测评方案	（1）要素齐全、格式正确、内容符合逻辑； （2）文档规范，无错别字、格式错误、语句不通顺等问题； （3）等保测评方法科学、合理。	20 分
5		等保测评问题报告单	（1）准确记录问题类型、问题描述，必要时，提供问题截图、安全整改建议； （2）等保测评问题报告单提交完整、及时。	10 分

6		等保测评报告	（1）要素齐全、格式正确、内容符合逻辑； （2）文档规范，无错别字、格式错误、语句不通顺等问题； （3）等保测评结果准确、合理。	15 分
7	服务评价扣分项	重大错误	在测评阶段出现失误，造成系统故障。	12 分
8		内容错误	等保测评内容不充分，未能完全执行第三方等保测评方案的等保测评内容。	8 分
9		一般错误	等保测评成果文档存在错别字和名称、编号、日期错误，以及编写格式不规范等。（发现 1 次扣 0.5 分，扣完为止）	5 分
10	否决项	重大及以上安全事件	出现故意泄露工作中掌握的相关保密信息、删除业务数据、密码泄露、传播病毒、故意损坏主机等重大安全事故。	出现一次重大及以上安全事件，甲方有权终止合同。
合计				100 分

服务款项结算标准

序号	评价分数范围	评价等级	支付比例
1	90 分≤评价≤100 分	优秀	100%
2	75 分≤评价<90 分	良	90%
3	60 分≤评价<75 分	中等	70%
4	评价低于 60 分	不合格	50%

备注：

1．服务结算标准是依据服务质量评价结果确定的服务费的支付比例。

2．上述结算标准仅作为甲方对乙方的服务质量评价结算标准，不作为验收条件。

3．计算公式：服务金额=合同总金额*评价分数对应的支付比例。

附件 1-3

廉洁承诺书

为加强商务活动中的廉政建设，防止发生各种谋取不正当利益的违法违纪行为、规范合同双方的各项活动，保障顺畅、公平的商业秩序，保护当事人的合法权益，根据《中华人民共和国民法典》等相关法律，我司承诺以下廉政责任：

一、我司承诺在与甲方的商务往来活动中遵循自愿、公平、等价有偿、诚实信用原则，并保证在合同订立、履行过程中以及事前事后保持公开、公平、公正、诚信、透明的原则，不会为获取不正当的利益，损害国家、集体和甲方利益。

二、我司保证我司以及我司工作人员与甲方保持正常的业务交往，按照有关法律法规的规定和程序开展业务活动，并遵守以下规定：

（一）不以任何理由向甲方工作人员提供或赠送礼金、有价证券、贵重物品及回扣、好处费、感谢费等。

（二）不以任何理由为甲方工作人员报销应由甲方工作人员个人支付的费用。

（三）不接受或暗示为甲方工作人员在装修住房、婚丧嫁娶、配偶子女的工作安排以及出国（境）、旅游等方面提供便利。

（四）不为甲方工作人员提供通信工具、交通工具和高档办公用品等物资。

（五）不以任何理由为甲方工作人员组织有可能影响廉洁、公正的宴请、健身、娱乐活动。

（六）不许诺事后给予甲方工作人员利益。

（七）不以其他手段为甲方工作人员提供其他不正当利益。

（八）上述条款中所称不正当利益包括但不限于金钱和实物。如回扣、佣金、股份、股东资格、债券、促销费、赞助费、广告宣传费、劳务费、红包、礼金、含有金额的会员卡、代币卡（券）、旅游费用、就业机会、项目机会、各种高档生活用品、奢侈消费品、工艺品、收藏品、房屋、车辆、减免债务、提供担保、免费娱乐、旅游、考察、提供房屋装修、借贷款项、借用物品、特殊待遇等财产性或者非财产性利益等。

三、我司同意，如违反以上约定，甲方有权终止合同，相关的责任由我司承担；涉嫌犯罪的，甲方有权移交司法机关，并追究刑事责任。若因此给甲方造成经济损失

的，我司同意按有关规定予以赔偿。

承诺方（盖章）：_____

签字日期：____年___月___日

附件 1-4

保密承诺书

根据《中华人民共和国保守国家秘密法》及有关规定，为保护项目涉及的工作或敏感信息，在遵循平等自愿、诚实信用的原则下，经协商一致，乙方就在履行本项目合同义务期间（以下简称“项目”）的保密事项，签订本承诺书，接受本承诺书的约束。

一、保密范围和内容

乙方通过参与甲方项目知晓的，以及在项目实施过程中产生的国家秘密、工作秘密或内部、敏感的信息和数据，包括但不限于：

（一）商业信息

1.承诺方在项目实施过程中了解的甲方单位性质、人员信息、工作内容、机构设置、责任分工、联系方式等信息；

2.承诺方知晓的甲方与其他公司的洽谈、合作、约定、协议、合同等信息。

（二）项目信息

1.项目相关应用系统业务需求、设计和实施方案、图纸、施工文档、测试报告、业务系统数据等信息；

2.甲方在项目实施过程中签署的会议纪要、谈判记录、招投标文件、合同书、变更、补充协议、往来函件等其他信息；

3.甲方设备安装场地、基础设施、机房、网络拓扑结构及其相关资料；

4.所涉及甲方信息系统的对接、漏洞、接口等信息；

5.甲方安全机制、安全系统，备份策略、应急演练及应急预案等；

6.项目其他相关文件、资料、技术文档、声像资料等。

（三）数据信息

1.项目相关设备数量、型号、配置、安装地点、运行状况等信息；

2.项目实施相关软件需求、设计文件、软件架构、源代码和可执行代码、程序文档、数据库、数据备份等资料；

3.项目实施所产生的所有数据（包括原始数据、过程数据、结果数据、日志数据、运维过程中产生的数据或信息等）及数据应用；

4.承诺方为甲方实施项目而通过其他渠道获取的与项目有关的数据信息；

5.其他经甲方确定或法律规定为国家秘密、工作秘密或内部、敏感的信息的所有事

项。

二、乙方及其工作人员保密义务

乙方及其工作人员只能为项目工作目的使用甲方的项目资料，且仅限于项目管理人员及直接参与项目工作的人员知悉，不得扩大知悉范围、泄露给任何第三方或作与项目无关的使用。在项目实施过程中，承诺方及其工作人员应当遵守甲方关于项目人员、项目信息载体、项目场所与设备、项目管理等相关规定，包括但不限于：

1.乙方应当对承诺约定的保密文档妥善保管，并对参与项目的人员及其分工作出详细文字记录，由项目保密员统一管理。

2.乙方需要与其他单位合作完成项目的，应征得甲方书面同意，并保证合作单位具有相应资质。

3.乙方应当与参与项目的人员分别签订一份保密承诺，该承诺的实质内容应当与本承诺内容相一致，未签署保密承诺的人员不得参与项目。

4.乙方应当对参与项目人员进行有效地管理。定期进行保密教育、培训和保密自查，及时发现和纠正项目保密工作的偏差，对违反保密规定的人员及时处理，并通报甲方。乙方参与项目的人员在项目实施过程中离职的，乙方应当立即将该情况通知甲方，并要求离职人员清理和移交本人保管的资料、文件、数据等含有项目信息的载体，离职人员需继续遵守该保密承诺。

5.乙方项目实施场地必须满足项目实施要求，实行严格的管理制度。在甲方场所内办公的，遵守甲方管理要求，不得接触与项目无关的信息，不得获取和掌握甲方各系统的用户名和密码，对于项目相关数据、信息未经允许不得私自存储、拷贝、复印、带离等。

6.乙方不得泄露甲方与乙方或与其他任何第三方的谈判合作信息等商业信息。

7.禁止将与项目有关的信息上传到互联网网站、论坛、网盘和社交媒体等，确需由邮件形式发送的必须加密处理。

8.项目的设计方案、研发成果及有关建设情况，不得擅自以任何形式公开发表、交流或转让、申请专利或申报国家奖励。

9.未经甲方书面许可，乙方不得使用甲方案例用于宣传、投标、技术交流等。

10.未经甲方书面许可，乙方不得留存甲方任何数据信息，不得以任何方式私自对项目有关数据的任何版本进行分析、加工、处理，不得以任何形式提供给其他第三方。

11.乙方不得泄露包括专利技术、技术秘密、产品信息、客户信息等甲方任何无形

资产。

12.对于乙方在本承诺生效之前或承诺终止后，通过保密承诺任何途径知悉或取得的有关甲方的重要信息，在本承诺生效后，乙方应当参照承诺履行相应的保密义务。

13.乙方在本承诺中承担的保密义务，不因本项目的中止或终止而解除。

14.乙方所邀请的第三方专业测试人员、技术支撑人员、相关厂商支持等外援人员，将严格按照项目相关要求开展项目工作，未经甲方书面同意，绝不随意传播项目信息。技术支持工作结束后，乙方需严格监督其妥善移交相关文件资料，绝不擅自销毁或另作他用。如因第三方人员问题产生的信息泄露，由乙方承担主要责任。

15.如因乙方技术、管理等原因，发生数据泄露、损坏、遗失，乙方必须承担相应赔偿等责任。

三、人员登记制度

乙方所有参与项目的人员应当保证履行本承诺约定的各项义务，如实填写“项目人员名单”，且每页加盖单位公章方为有效。乙方对其工作人员登记信息的真实性负责。在项目实施过程中增加的人员，乙方应当在人员入场前追加填写“项目人员名单”。原厂实施人员，应当同时加盖原厂单位公章和乙方公章方为有效。乙方应当按照国家相关保密管理规定，严格禁止除登记人员以外的人员知悉项目的一切信息。乙方应当对参与政府信息化建设的关键数据岗位人员开展必要的安全背景审查，确保数据安全。

四、工作联系

为落实好本承诺，乙方应当采取必要的措施防止任何泄密情况的发生，并指定专人负责双方之间的保密工作关系，并随时就本承诺的保密事宜进行研究和落实，乙方特选派_____为专项联系人。

五、通知

乙方发现有失密、泄密、窃密等行为发生的，应当立即通知甲方，并应当密切协作，尽快查明事件原因、过程、后果等情况。

六、保密期限

乙方的保密义务为无限期保密，即从本承诺签订之日起承担保密义务。

七、争议解决

本承诺条款，如存在与国家有关法规相抵触，按照国家有关法规执行，双方若发生争议，应当首先友好协商解决，协商不成，任何一方均可向甲方住所地人民法院提起诉讼。

八、其他要求

1.双方就项目所签订的合同变更、解除或提前终止的，本承诺效力不受影响。

2.未经甲方和乙方双方事先书面达成一致意见，本承诺书不得以任何其他理由而更改。

承诺方（盖章）：_____

日期：_____年___月___日

合同登记编号：

局属信息系统密码应用安全性评估项目合同（F 包）

项目名称：_____

委托方（甲方）：_____

受托方（乙方）：_____

签订地点：_____河南郑州_____

局属信息系统密码应用安全性评估项目

服务合同

甲方：

乙方：

按照《中华人民共和国民法典》《中华人民共和国政府采购法》，经 _____（以下简称甲方）和中标单位_____（以下简称乙方）在友好协商、平等互惠的基础上，就甲方委托乙方承担局属信息系统密码应用安全性评估项目的有关事项达成一致意见，签订本合同，经双方确认，一致同意以下条款，以资共同遵守：

第一条 术语和定义

在本合同中，下列术语及定义，除上下文另有约定外，应具有本条所赋予的含义。

1.1 “一方”：指甲方或乙方中的任何一方。

1.2 “双方”：指甲方和乙方。

1.3 “合同”：指双方就本项目达成并签署的协议，包括所有的附件，以及下面指出的构成合同的所有文件。双方同意下列文件作为本合同不可分割的组成部分：

1.3.1 本合同正文；

1.3.2 本合同附件；

1.3.3 在本合同履行过程中双方共同签署的补充与修正文件。

1.4 “合同总价”：指根据合同规定，在乙方全面正确地履行合同义务时甲方应支付给乙方的总金额。包括完成本项目所需的服务费、人工费、交通费、食宿费、工具购置费、测试费、税费、验收费等完成本项目全部内容所需的所有费用。

1.5 “工作日”：即标准工作日，指国家所规定的节假日之外的所有工作日，未指明为工作日的日期指自然顺延的日期。

1.6 “信息系统”：是由计算机硬件、网络和通信设备、计算机软件、信息资源、信息用户和规章制度组成的以处理信息流为目的的人机一体化系统。

1.7 “秘密”：指甲方所拥有的，不为公众所知的管理信息、方式方法、用户名单、数据、信息、技术诀窍、源代码、计算机文档等，或由双方在履行本合同过程中明确指明为秘密的、法律所认可的任何信息。

1.8 “重大故障”：指乙方在测评服务过程中，由于失责或操作不当导致应用系统整体运行中断无法正常使用并且不能够在 4 小时以内解决的故障问题。

1.9 “附件”：指与本合同的订立、履行有关的，经双方书面认可的，对本合同约定的内容进行细化、补充、修改、变更的文件、图纸、音像制品等资料。

第二条 本项目合同组成

本项目合同由双方协商并载入本合同中的条款、条件，磋商文件、应答文件、成交通知书以及所提及的附件和有关的补充协议构成。本合同构成文件间有矛盾时，以日期在后的文件为准；双方同意在出现合同理解上的歧义时，按照有利于甲方的原则执行。

第三条 服务期间和服务地点

3.1 技术服务期限

3.1.1 合同签订生效后至_____年_____月_____日。

3.1.2 具备评估条件之日起____个工作日内完成现场评估。

3.2 技术服务地点

河南省郑州市或甲方指定的其他地点。

3.3 服务方式

3.3.1 以文字报告的方式提供服务。

3.3.2 安排相关技术人员提供现场评估服务。

第四条 服务内容和范围

4.1 甲方委托乙方提供本项服务工作，乙方承诺为甲方提供商用密码应用安全性评估服务：

序号	局属信息系统分项名称	等保等级
1	河南省“豫正通”	三级
2	河南省大数据中心(一期)	三级
3	河南省一体化协同办公平台	三级

4.1.1 按照商用密码应用安全性评估最新要求，对甲方的被测系统进行测评。

4.1.2 汇总、整理和分析测评结果，提出相应整改建议，协助甲方开展系统安全整改工作。

4.1.3 按照甲方要求，协助完成系统备案等工作。

4.1.4 按照甲方要求，并结合实际工作需要，必要时调整被测系统定级级别，以最终实际定级、备案级别为准。

4.2 服务阶段

4.2.1 分为测评准备阶段、方案编制阶段、现场测评阶段（含复测）、分析与报告编制阶段。

4.2.2 各阶段需交付的测评过程文档按照项目招标文件要求提供。

4.3 服务机构、职责与人员配备安排：

4.3.1 乙方按照服务内容和目标要求成立商用密码应用安全性评估服务小组。服务小组在项目经理领导下，按照项目要求和目标任务确定工作职责，于项目启动后 1 日内建立健全各项规章制度。

4.3.2 乙方根据项目要求和甲方需要配备有关专业人员，提供 1 名项目经理具有信息系统项目管理师证书和信息安全保障人员（CISAW）认证考核证书。不少于_____名测评人员，通过商用密码应用安全性评估人员测评能力考核且具备三年以上测评经验（以取得证书的时间为准）。

第五条 服务要求

5.1 乙方应严格建立质量保证体系，制定项目建设的质量控制方案和实施措施，并督促完成各环节质量控制内容和目标；保证项目各个阶段满足甲方对质量的要求。

5.2 乙方应根据项目的工作计划，对阶段性项目工作成果进行审核，并向甲方提交里程碑式工作成果。通过保证各阶段性成果的质量，最终保证整个项目的质量。

5.3 所有提交给甲方的技术报告及相关资料的最后文本，包括为履行技术服务范围所编制的图纸、计划和证明资料等，都属于甲方的财产，乙方在提交给甲方之前应将上述资料进行整理归类和编制索引。

5.4 未经甲方的书面同意，乙方不得将上述资料本服务项目之外的任何项目。

第六条 服务标准

6.1 依据GB/T 39786-2021《信息系统密码应用基本要求》、GB/T 43206-2023 《信息安全技术 信息系统密码应用测评要求》、GM/T 0116-2021《信息系统密码应用测评过程指南》、《信息系统高风险判定指引》和系统自身的安全需求分析，对被评估系统进行商用密码应用安全性评估，为被测系统的商用密码安全提供科学评价，逐步规范网络运营者的密码使用和管理行为。在商用密码应用安全性评估完成后，提交《商用密码应用安全性评估报告》到当地密码管理局和采购人。

6.2 实施方式

系统评估，及时发现系统脆弱性，识别变化的风险，了解系统安全状况。对照密码应用方案对系统开展评估。根据被评估对象的实际情况、所属行业及系统使用的密码产品情况，选择并确定测评依据。在系统真实环境下进行测评，以评估密码保障是否安全有效，密码使用是否合规、正确、有效。并通过测评发现系统存在的安全隐患和风险，提出可行性完善建议。

6.3 需遵循的政策法规及行业规范：依据标准

信息系统密码安全服务全过程所有工作严格按照最新国家相关安全标准执行，以保证服务工作科学、规范地进行，具体参考的标准如下：

《GB/T 39786-2021信息系统密码应用基本要求》

《GB/T 43206-2023 信息安全技术 信息系统密码应用测评要求》

《GM/T 0116-2021信息系统密码应用测评过程指南》

《商用密码应用安全性评估管理办法》

《信息系统密码应用高风险判定指引》

《政务信息系统密码应用与安全性评估工作指南》2020版

《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知（国办发〔2019〕57号）》

《国家密码管理局关于请进一步加强国家政务信息系统密码应用与安全性评估工作的函（国密局函〔2020〕119号）》。

第七条 双方的权利与义务

7.1 甲方的权利和义务

7.1.1 甲方应当依据本合同的约定，向乙方支付测评服务价款。

7.1.2 甲方为乙方提供本合同项下所需要的资源，包括访问测评范围内网络设备和主机设备的权限及其他相关资料。

7.1.3 甲方确保乙方实施本合同项下的服务时，对于设备的使用、信息的获取和更改，不会违反任何保密或协议责任，不会侵犯第三方的权利。

7.1.4 甲方有权在乙方履行合同过程中出现损害或可能损害国家利益、公共利益、公共安全情形时变更、中止或者终止本合同。

7.1.5 甲方授权河南省政务大数据中心作为受委托方，负责项目运维服务过程中的技术性管理工作，具体包括：项目需求统筹，技术方案审核，项目安全保障和应急处置，

对乙方提供的服务进行考核，对乙方服务质量进行监督，组织参与项目验收。

7.2 乙方的权利和义务

7.2.1 乙方应当按照甲方的要求，制定适用于本合同服务范围的内部质量和风险控制制度及措施，确保完成本项目的测评服务。

7.2.2 乙方人员在项目执行期间应保持相对稳定，以保证项目的顺利实施。乙方人员的变更需提前 3 日向甲方提出书面申请，并保证接替人员能够胜任此项测评工作，经甲方书面同意后方可变更，变更时做好该项目的技术及文档交接。参与项目的所有人员都应当受本合同各条款的约束。

7.2.3 乙方须确保乙方及项目组人员遵守附件 3《保密承诺书》的各项内容。

7.2.4 乙方按合同要求实施测评的过程中，应当及时向甲方通报在信息系统中发现的安全问题，并协助甲方尽可能地弥补缺陷。

7.2.5 乙方应当接受并配合甲方组织的对本合同履行情况的监督与检查，对于甲方指出的问题，应及时作出合理解释或予以纠正。

7.2.6 乙方应当根据甲方要求，接受和配合甲方或甲方委托机构进行的与本合同相关的审计。

7.2.7 乙方在项目实施过程中出现资源、进度、质量协调控制不力的情况，甲方有权要求更换相关项目人员，乙方必须予以配合，并确保不影响项目的进度和质量。

7.2.8 乙方应当根据服务的内容和进度安排，按时提交阶段性技术报告及有关资料。

7.2.9 乙方在实施关键测评项时，要与甲方充分沟通该关键测评项实施的细节与步骤，得到甲方许可后，再开展该测评，以该测评项对甲方的信息系统影响最小化为目标。

7.2.10 项目交付后，乙方应当无条件返还甲方提供的文件、资料，同时乙方应当自留一份完整的项目档案按保密信息标准予以妥善保存，以便质保工作的顺利开展，但不得用于第三方和其他项目。

第八条 项目验收

8.1 乙方服务完成后，向甲方提交验收申请，由甲方组织项目的验收工作，乙方在合同期满前提交以下项目文档：

8.1.1 提交被测系统的《商用密码应用安全性评估方案》；

8.1.2 提交被测系统的《商用密码应用安全性评估报告》。

8.1.3 根据测评中反映出的安全问题，汇总、整理、分析测评结果，按照适度有效

的原则，向甲方提交《商用密码应用安全性评估整改技术方案》；

8.2 甲方收到以上文档后，组织人员开展验收。

8.3 验收完毕后，乙方应持续协助甲方开展整改工作，对整改后的成效按验收标准进行评审，重新出具评估报告。

第九条 合同价款、支付方式及履约保证

9.1 本项目合同总价款为人民币小写：￥_____元，（含税价），人民币大写_____元整（含税价）。

9.2 首期款：签订合同后，乙方书面提交与拟支付金额等额的符合甲方财务管理要求的相应发票后____个工作日内，启动首期款支付流程，支付合同总金额的 30%，即人民币大写_____元整（￥_____元）。（如果支付款包含多项费用，应当按大类分别列出支出明细；如果支付的款项需要支付给不同的公司，要按公司分别支付，以下同。）

9.3 尾款：经甲方确认验收合格后，依据绩效评估结果计算金额扣除已支付金额以及违约金额计算支付，甲方在收到乙方书面提交支付申请函及拟支付金额等额的符合甲方财务管理要求的相应发票后__个工作日内，启动尾款支付流程，即人民币大写_____元整（￥_____元）。

9.4 乙方在甲方支付合同款项前，应先按各期付款数额在 10 个工作日内向甲方开具符合国家法律法规和标准的税务发票，之后甲方按程序向乙方进行支付。若乙方未提供合法有效的发票，甲方有权拒付款项，且不承担违约责任。

第十条 合同变更

10.1 如本合同在履行过程中有任何变更、补充或修改，都必须经甲乙双方协商同意，必要时依据重要程度由双方法定代表人或授权代表另行签订书面协议。

10.2 甲方提出变更要求

10.2.1 如甲方要求变更项目服务内容，应当以书面形式将相关要求提交给乙方。乙方应当在 7 个工作日内，对该变更后在项目交付日期、工作量、影响范围等方面做出评估，并书面回复甲方。

10.2.2 甲方在收到乙方回复后，应当在 7 个工作日内，以书面方式通知乙方，对是否接受进行回复。因甲方提出的变更导致工作量增加的，如果增加的工作量不超过总量的 20%，则合同总价不作调增；因甲方提出的变更导致工作量减少的，如果减少工作量不超过总量的 20%（含），则合同总价不作调减。如果增加工作量超过总量的 20%，

甲方将视增加的服务为新项目，另行立项。如果减少工作量超过总量的20%，经双方共同协商后，签订补充协议，按比例调整合同总价。

10.2.3 合同履行期间甲方因业务职能或重大政策发生变更或因其他原因导致合同无法继续履行时，甲方有权解除本合同，且不承担任何违约责任。合同未履行部分的费用不再支付，已支付部分按未实施的服务部分比例或剩余服务时间的比例进行返还，未支付部分按已实施的服务部分时长与全年时长比例进行支付。

10.3 乙方提出变更建议

10.3.1 如乙方要求变更项目服务内容，乙方应当对该变更后在项目交付日期、工作量、影响范围等方面做出评估，并以书面形式提交给甲方。

10.3.2 甲方在收到乙方的变更建议后，应当在7个工作日内，以书面方式通知乙方是否接受乙方的变更建议。如甲方接受乙方的变更建议，因乙方提出的变更导致工作量增加的，则合同总价不做调增；因乙方提出的变更导致工作量减少的，如果减少工作量不超过总量的20%（含），则合同总价不做调减。如果减少工作量超过总量的20%，则经双方共同协商后，签订补充协议，按比例调整合同总价。

第十一条 知识产权

11.1 乙方在履行和完成本合同项下工作过程中准备及形成的一切资料，包括但不限于文件、计算方法、图表、报告、数据、模型和样品，以及其中含有的所有发明为甲方所有，甲方有权使用上述资料以履行本项目合同或用于其他目的。该资料应与本项目合同项下其他资料一起，按要求在本项目合同结束或终止的时候，交还给甲方。

11.2 本项目所形成的产品其知识产权归甲方所有，乙方非经甲方书面同意，不得以任何方式向第三方披露或转让。除本项目测评需要外，乙方不得以任何方式在任何情形下利用。

11.3 涉及乙方的测试流程、测试方法、分析方法、方案模板、报告模板等相近知识产权内容归乙方所有。

第十二条 保密

乙方须与甲方签订保密承诺书作为合同附件，见附件3。

第十三条 违约责任及损失赔偿

13.1 如果乙方在工作中发生重大及以上安全事件，包括但不限于由于乙方故意或过失等原因造成甲方系统出现重大网络中断、数据丢失、系统瘫痪或者出现反动言论等情况或者因测评不符合合同要求，严重影响到甲方正常的业务工作，甲方有权决定是否

解除合同，乙方须承担由此给甲方带来的一切损失。

13.2 乙方违反合同约定的保密义务，乙方应当支付合同总价 1%的违约金。如实际损失超过违约金的，甲方有权要求对方赔偿超过部分。

13.3 任何一方违反合同约定的知识产权保护条款，除立即停止违约行为外，还应当支付合同价款的 1%作为违约金。

13.4 乙方工作人员未经甲方授权，擅自篡改甲方业务数据，或利用甲方现有业务信息系统、网络平台或者冒用甲方身份获取非法利益，造成甲方或任何第三方损失的，由乙方承担法律责任并负责赔偿全部损失，同时乙方须向甲方支付本合同总价款 1%的违约金。

13.5 因乙方原因造成严重超期、拖延而不能按时交付，自交付日期起，每超期一周乙方应当支付合同总价 1%的违约金。

13.6 如乙方工作人员擅自承担或参与涉及甲方职能的行政业务工作，对甲方造成不良影响的，乙方应立即停止其行为并采取发布声明等措施消除影响，同时甲方保留追究乙方法律责任的权利。

13.7 如乙方发生违约事件，甲方要求乙方支付违约金或赔偿款时，应当以书面方式通知乙方，内容包括违约事件、违约金、支付时间和方式等。乙方在收到上述通知后，应当于 7 日内答复甲方，并支付违约金或赔偿金。逾期未支付的，甲方有权在合同款项中予以扣除。

13.8 服务期限内，如乙方发生违约事件累计超过三次，甲方有权单方终止合同，并将乙方列入不良行为记录，甲方有权限制乙方参与甲方此后的测评服务项目。

第十四条 不可抗力

14.1 本合同中不可抗力系指甲乙双方在缔结合同时所不能预见的、并且其发生及其后果是无法避免和无法克服的客观情况。

14.2 由于不可抗力致使合同无法履行的，受不可抗力影响一方应立即将不能履行本合同的事实书面通知对方，并协助对方最大可能减少损失，在不可抗力发生之日起 7 日内提供有关政府部门或公证机关出具的证明文件。

14.3 本合同在不可抗力影响范围及其持续期间内将中止履行，本合同执行时间可根据中止的时间相应顺延，双方无需承担违约责任。不可抗力事件消除后，双方应当就合同的履行及后续问题进行协商。

第十五条 合同转让及终止

15.1 合同转让：非经双方书面同意，任何一方无权转让本合同及该合同约定的全部或部分权利、义务。非经对方同意擅自转让的，对方有权解除合同，并要求擅自转让方承担全部赔偿责任。

15.2 合同终止

15.2.1 合同自然终止：甲乙双方全部履行合同约定的义务后，本合同自然终止。

15.2.2 违约合同终止：若合同一方有足够证据证明合同另一方未在规定时间内履行本合同项下规定义务，可向对方提出书面违约通知，提出终止部分或全部合同，合同中未终止的部分应继续履行。

15.2.3 无能力履行合同终止：如有充分证据证明乙方无清偿能力或无继续履行合同的能力，甲方可以在任何时候以书面形式通知对方，提出终止合同而不给对方补偿，或要求资产保全防止损失扩大。

15.3 双方协商一致可以终止合同。

第十六条　适用法律及争议解决

16.1 本合同按中华人民共和国法律解释。

16.2 甲、乙双方在合同履行过程中发生的一切争议，均应通过双方友好协商解决；协商不成的，任何一方均可向甲方住所地人民法院提起诉讼。

16.3 在诉讼期间，除正在进行诉讼的部分外，本合同的其他部分应当继续执行。

第十七条 合同的生效

17.1 本合同经双方盖章以及法定代表人或授权代表签字后生效。

17.2 本合同一经签署，未经双方书面同意，任何一方不得随意更改。

17.3 本合同一式肆份，甲乙双方各执贰份，具有同等法律效力。

第十八条 其他

18.1 如一方改变通讯地址及其他信息，应当在变更后 7 日内以书面方式通知另一方，否则，由此而造成的损失，由信息发生变更的一方承担。

18.2 本合同未尽事宜，双方可以另行协商签订补充协议，补充协议经双方盖章以及法定代表人或授权代表签字后生效与本合同具有同等效力。

（以下无正文，仅为签章页）

甲方（盖章）：_____

法定代表人或授权代表（签字）：_____

统一社会信用代码：_____

联系人：_____

联系电话：_____

地址：_____

2026 年　月　日

乙方（盖章）：_____

法定代表人或授权代表（签字）：

统一社会信用代码:_____

开户银行及账号：_____

联系人：_____

联系电话：_____

地址：_____

2026 年　月　日

附件 1-1

项目人员名单

职务	姓名	职称	执业或职业资格证明				备注
			证书名称	级别	证号	专业	
项目负责人							
技术负责人							
项目支撑							
质量管理							
项目组成员							
项目组成员							
项目组成员							
项目组成员							
项目组成员							
项目组成员							
项目组成员							
项目组成员							
项目组成员							

附件 1-2

绩效考核标准

序号	评价指标	评分内容	分值
1	评估报告	根据甲方要求，按时完成评估报告编制并交付。如工作不及时或不满足需求扣 1 分，直到扣完为止。	10 分
2	人员管理	确保人员稳定性，未经过甲方同意现场人员随意变动，扣 1 分；出现人员技术能力（资质）达不到合同要求情况，扣 5 分，直到扣完为止。	10 分
3	服务质量	服务过程中各项工作完成及时，质量符合要求，出现不满足甲方工作要求的任务交付，每次扣 2 分。	20 分
4	响应及时性	工作时间：在合同约定的工作时段内，必须确保电话畅通，及时接听甲方人员电话通知 5 分钟内响应，否则视为非及时响应，每发生一起非及时响应扣 3 分； 非工作时间：在非工作时段，应确保 24 小时电话开机。在需要紧急服务支撑时，在接到甲方人员通知后 30 分钟内赶到现场视为及时，否则视为非及时响应。每发生一起非及时响应扣 2 分。	20 分
5	备案服务	项目服务期间根据甲方要求，完成系统的备案材料梳理及当地密码管理局备案工作，如出现因乙方原因导致服务结果不满足备案工作要求的任务交付，每次扣 2 分。	10 分
6	密码评估服务	项目服务期间根据甲方要求，完成系统的商用密码应用安全性评估工作，如出现因乙方原因导致服务结果不满足工作要求的任务交付，每次扣 2 分。	10 分
7	过程管理	1.项目服务期间根据甲方要求对服务过程所涉及的文档进行管理并按进度交付，如出现未按时间节点提交相关过程文档的情况，每次扣 2 分。	20 分

		2.项目服务期间，涉及上机验证操作或需进行工具检测项目，需在提交详细实施方案的同时明确应急响应措施，如出现因乙方原因导致被测评系统运行故障的情况，每次扣5分。	
8	否决项	出现故意泄露工作中掌握的相关保密信息、删除业务数据、密码泄露、传播病毒、故意损坏主机等重大安全事件。	出现一次重大及以上安全事件，甲方有权终止合同。
合计			100分

服务款项结算标准

序号	评价分数范围	评价等级	支付比例
1	90分≤评价≤100分	优秀	100%
2	75分≤评价<90分	良	90%
3	60分≤评价<75分	中等	70%
4	评价低于60分	不合格	50%

备注：

1．服务结算标准是依据服务质量评价结果确定的服务费的支付比例。

2．上述结算标准仅作为甲方对乙方的服务质量评价结算标准，不作为验收条件。

3．计算公式：服务金额=合同总金额*评价分数对应的支付比例。

附件 1-3

廉洁承诺书

为加强商务活动中的廉政建设，防止发生各种谋取不正当利益的违法违纪行为、规范合同双方的各项活动，保障顺畅、公平的商业秩序，保护当事人的合法权益，根据《中华人民共和国民法典》等相关法律，我司承诺以下廉政责任：

一、我司承诺在与甲方的商务往来活动中遵循自愿、公平、等价有偿、诚实信用原则，并保证在合同订立、履行过程中以及事前事后保持公开、公平、公正、诚信、透明的原则，不会为获取不正当的利益，损害国家、集体和甲方利益。

二、我司保证我司以及我司工作人员与甲方保持正常的业务交往，按照有关法律法规的规定和程序开展业务活动，并遵守以下规定：

（一）不以任何理由向甲方工作人员提供或赠送礼金、有价证券、贵重物品及回扣、好处费、感谢费等。

（二）不以任何理由为甲方工作人员报销应由甲方工作人员个人支付的费用。

（三）不接受或暗示为甲方工作人员在装修住房、婚丧嫁娶、配偶子女的工作安排以及出国（境）、旅游等方面提供便利。

（四）不为甲方工作人员提供通信工具、交通工具和高档办公用品等物资。

（五）不以任何理由为甲方工作人员组织有可能影响廉洁、公正的宴请、健身、娱乐活动。

（六）不许诺事后给予甲方工作人员利益。

（七）不以其他手段为甲方工作人员提供其他不正当利益。

（八）上述条款中所称不正当利益包括但不限于金钱和实物。如回扣、佣金、股份、股东资格、债券、促销费、赞助费、广告宣传费、劳务费、红包、礼金、含有金额的会员卡、代币卡（券）、旅游费用、就业机会、项目机会、各种高档生活用品、奢侈消费品、工艺品、收藏品、房屋、车辆、减免债务、提供担保、免费娱乐、旅游、考察、提供房屋装修、借贷款项、借用物品、特殊待遇等财产性或者非财产性利益等。

三、我司同意，如违反以上约定，甲方有权终止合同，相关的责任由我司承担；涉嫌犯罪的，甲方有权移交司法机关，并追究刑事责任。若因此给甲方造成经济损失的，我司同意按有关规定予以赔偿。

承诺方（盖章）：_____

签字日期：_____年___月___日

附件 1-4

保密承诺书

根据《中华人民共和国保守国家秘密法》及有关规定，为保护项目涉及的工作或敏感信息，在遵循平等自愿、诚实信用的原则下，经协商一致，乙方就在履行本项目合同义务期间（以下简称“项目”）的保密事项，签订本承诺书，接受本承诺书的约束。

一、保密范围和内容

乙方通过参与甲方项目知晓的，以及在项目实施过程中产生的国家秘密、工作秘密或内部、敏感的信息和数据，包括但不限于：

（一）商业信息

1.承诺方在项目实施过程中了解的甲方单位性质、人员信息、工作内容、机构设置、责任分工、联系方式等信息；

2.承诺方知晓的甲方与其他公司的洽谈、合作、约定、协议、合同等信息。

（二）项目信息

1.项目相关应用系统业务需求、设计和实施方案、图纸、施工文档、测试报告、业务系统数据等信息；

2.甲方在项目实施过程中签署的会议纪要、谈判记录、招投标文件、合同书、变更、补充协议、往来函件等其他信息；

3.甲方设备安装场地、基础设施、机房、网络拓扑结构及其相关资料；

4.所涉及甲方信息系统的对接、漏洞、接口等信息；

5.甲方安全机制、安全系统，备份策略、应急演练及应急预案等；

6.项目其他相关文件、资料、技术文档、声像资料等。

（三）数据信息

1.项目相关设备数量、型号、配置、安装地点、运行状况等信息；

2.项目实施相关软件需求、设计文件、软件架构、源代码和可执行代码、程序文档、数据库、数据备份等资料；

3.项目实施所产生的所有数据（包括原始数据、过程数据、结果数据、日志数据、运维过程中产生的数据或信息等）及数据应用；

4.承诺方为甲方实施项目而通过其他渠道获取的与项目有关的数据信息；

5.其他经甲方确定或法律规定为国家秘密、工作秘密或内部、敏感的信息的所有事项。

二、乙方及其工作人员保密义务

乙方及其工作人员只能为项目工作目的使用甲方的项目资料，且仅限于项目管理人员及直接参与项目工作的人员知悉，不得扩大知悉范围、泄露给任何第三方或作与项目无关的使用。在项目实施过程中，承诺方及其工作人员应当遵守甲方关于项目人员、项目信息载体、项目场所与设备、项目管理等相关规定，包括但不限于：

1.乙方应当对承诺约定的保密文档妥善保管，并对参与项目的人员及其分工作出详细文字记录，由项目保密员统一管理。

2.乙方需要与其他单位合作完成项目的，应征得甲方书面同意，并保证合作单位具有相应资质。

3.乙方应当与参与项目的人员分别签订一份保密承诺，该承诺的实质内容应当与本承诺内容相一致，未签署保密承诺的人员不得参与项目。

4.乙方应当对参与项目人员进行有效地管理。定期进行保密教育、培训和保密自查，及时发现和纠正项目保密工作的偏差，对违反保密规定的人员及时处理，并通报甲方。乙方参与项目的人员在项目实施过程中离职的，乙方应当立即将该情况通知甲方，并要求离职人员清理和移交本人保管的资料、文件、数据等含有项目信息的载体，离职人员需继续遵守该保密承诺。

5.乙方项目实施场地必须满足项目实施要求，实行严格的管理制度。在甲方场所内办公的，遵守甲方管理要求，不得接触与项目无关的信息，不得获取和掌握甲方各系统的用户名和密码，对于项目相关数据、信息未经允许不得私自存储、拷贝、复印、带离等。

6.乙方不得泄露甲方与乙方或与其他任何第三方的谈判合作信息等商业信息。

7.禁止将与项目有关的信息上传到互联网网站、论坛、网盘和社交媒体等，确需由邮件形式发送的必须加密处理。

8.项目的设计方案、研发成果及有关建设情况，不得擅自以任何形式公开发表、交流或转让、申请专利或申报国家奖励。

9.未经甲方书面许可，乙方不得使用甲方案例用于宣传、投标、技术交流等。

10.未经甲方书面许可，乙方不得留存甲方任何数据信息，不得以任何方式私自对项目有关数据的任何版本进行分析、加工、处理，不得以任何形式提供给其他第三方。

11.乙方不得泄露包括专利技术、技术秘密、产品信息、客户信息等甲方任何无形资产。

12.对于乙方在本承诺生效之前或承诺终止后，通过保密承诺任何途径知悉或取得的有关甲方的重要信息，在本承诺生效后，乙方应当参照承诺履行相应的保密义务。

13.乙方在本承诺中承担的保密义务，不因本项目的中止或终止而解除。

14.乙方所邀请的第三方专业测试人员、技术支撑人员、相关厂商支持等外援人员，将严格按照项目相关要求开展项目工作，未经甲方书面同意，绝不随意传播项目信息。技术支持工作结束后，乙方需严格监督其妥善移交相关文件资料，绝不擅自销毁或另作他用。如因第三方人员问题产生的信息泄露，由乙方承担主要责任。

15.如因乙方技术、管理等原因，发生数据泄露、损坏、遗失，乙方必须承担相应赔偿等责任。

三、人员登记制度

乙方所有参与项目的人员应当保证履行本承诺约定的各项义务，如实填写“项目人员名单”，且每页加盖单位公章方为有效。乙方对其工作人员登记信息的真实性负责。在项目实施过程中增加的人员，乙方应当在人员入场前追加填写“项目人员名单”。原厂实施人员，应当同时加盖原厂单位公章和乙方公章方为有效。乙方应当按照国家相关保密管理规定，严格禁止除登记人员以外的人员知悉项目的一切信息。乙方应当对参与政府信息化建设的关键数据岗位人员开展必要的安全背景审查，确保数据安全。

四、工作联系

为落实好本承诺，乙方应当采取必要的措施防止任何泄密情况的发生，并指定专人负责双方之间的保密工作关系，并随时就本承诺的保密事宜进行研究和落实，乙方特选派_____为专项联系人。

五、通知

乙方发现有失密、泄密、窃密等行为发生的，应当立即通知甲方，并应当密切协作，尽快查明事件原因、过程、后果等情况。

六、保密期限

乙方的保密义务为无限期保密，即从本承诺签订之日起承担保密义务。

七、争议解决

本承诺条款，如存在与国家有关法规相抵触，按照国家有关法规执行，双方若发生争议，应当首先友好协商解决，协商不成，任何一方均可向甲方住所地人民法院提起诉

讼。

八、其他要求

1.双方就项目所签订的合同变更、解除或提前终止的，本承诺效力不受影响。

2.未经甲方和乙方双方事先书面达成一致意见，本承诺书不得以任何其他理由而更改。

承诺方（盖章）：_____

签字日期：____年___月___日

合同登记编号：

局属信息系统综合安全监管项目合同
（G包）

项目名称：_____

委托方（甲方）：_____

受托方（乙方）_____

签订地点：_____河南郑州_____

局属信息系统综合安全监管项目

服务合同

甲方：

乙方：

按照《中华人民共和国民法典》《中华人民共和国政府采购法》，经_____（以下简称甲方）和中标单位_____（以下简称乙方）在友好协商、平等互惠的基础上，就甲方委托乙方承担局属信息系统综合安全监管项目的有关事项达成一致意见，签订本合同，经双方确认，一致同意以下条款，以资共同遵守：

第一条 术语和定义

在本合同中，下列术语及定义，除上下文另有约定外，应具有本条所赋予的含义。

1.1 “一方”：指甲方或乙方中的任何一方。

1.2 “双方”：指甲方和乙方。

1.3 “合同”：指双方就本项目达成并签署的协议，包括所有的附件，以及下面指出的构成合同的所有文件。双方同意下列文件作为本合同不可分割的组成部分：

1.3.1 本合同正文；

1.3.2 本合同附件；

1.3.3 在本合同履行过程中双方共同签署的补充与修正文件。

1.4 “合同总价”：指根据合同规定，在乙方全面正确地履行合同义务时甲方应支付给乙方的总金额。包括完成本项目所需的服务费、人工费、交通费、食宿费、工具购置费、测试费、税费、验收费等完成本项目全部内容所需的所有费用。

1.5 “工作日”：即标准工作日，指国家所规定的节假日之外的所有工作日，未指明为工作日的日期指自然顺延的日期。

1.6 “信息系统”：是由计算机硬件、网络和通信设备、计算机软件、信息资源、信息用户和规章制度组成的以处理信息流为目的的人机一体化系统。

1.7 “秘密”：指甲方所拥有的，不为公众所知的管理信息、方式方法、用户名单、数据、信息、技术诀窍、源代码、计算机文档等，或由双方在履行本合同过程中明确指明为秘密的、法律所认可的任何信息。

1.8 “重大故障”：指乙方在测评服务过程中，由于失责或操作不当导致应用系统

整体运行中断无法正常使用并且不能够在4小时以内解决的故障问题。

1.9 “附件”：指与本合同的订立、履行有关的，经双方书面认可的，对本合同约定的内容进行细化、补充、修改、变更的文件、图纸、音像制品等资料。

第二条 本项目合同组成

本项目合同由双方协商并载入本合同中的条款、条件，磋商文件、应答文件、成交通知书以及所提及的附件和有关的补充协议构成。本合同构成文件间有矛盾时，以日期在后的文件为准；双方同意在出现合同理解上的歧义时，按照有利于甲方的原则执行。

第三条 服务期间和服务地点

3.1 技术服务期限

3.1.1 合同签订生效后至____年____月____日。

3.2 技术服务地点

河南省郑州市或甲方指定的其他地点。

3.3 服务方式

3.3.1 以文字报告的方式提供服务。

3.3.2 安排相关技术人员提供现场测评服务。

第四条 服务内容和范围

4.1 **第一条 技术服务的内容、方式和要求**

4.1.1．技术服务内容：对省一体化政务服务平台（一期）、“豫事办”（一期）、省“豫正通”、省“互联网+监管”系统（一期）、省一体化协同办公平台、省电子政务外网管理中心（一期）、安全防护项目和内容安全监测项目的综合安全监管服务项目，通过常态化、全流程的综合安全监管服务，全面识别局属政务信息系统存在的安全漏洞，开展常态化渗透测试、新增功能上线前安全检查、安全审计、风险评估、安全漏洞复测、专项安全检查、安全咨询、安全培训等，提升系统整体安全防护能力，保障政务数据安全和业务稳定运行。（具体要求见附件）

4.1.2．技术服务方式：乙方到被体检系统所在地开展现场体检工作。

4.1.3．技术服务要求：乙方完成系统体检后，应按要求认真汇总分析工作情况，每个系统体检出具详细报告（或清单、制度、规范、预案等），并形成整体工作报告，及时提交给甲方。

4.2 售后服务要求。

4.2.1 乙方提供1年免费售后服务技术支持，提供7×24小时远程服务，必要时2

小时内到达现场提供紧急情况的应急支持服务，确保 8 小时内解决问题。

第五条 服务要求

依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》及网络安全等级保护 2.0 标准要求，通过对河南省一体化政务服务平台（一期）、河南省政务服务移动端“豫事办”(一期)、河南省“豫正通”、河南省“互联网+监管”系统（一期）、河南省一体化协同办公平台、河南省电子政务外网管理中心（一期）、安全防护项目、内容安全监测项目的综合安全监管服务，全面识别局属政务信息系统存在的安全漏洞，开展常态化渗透测试、新增功能上线前安全检查、安全审计、风险评估、安全漏洞复测、专项安全检查、安全应急响应、安全咨询和网络安全风险威胁情报收集等，提升系统整体安全防护能力，保障政务数据安全和业务稳定运行。

5.1 常态化渗透测试服务

供应商在授权和监督下，对指定的局属政务信息系统进行受控的、非破坏性的渗透测试，目的是侵入系统，获取系统控制权并将入侵的过程和细节生成报告给用户，发现用户系统所存在的安全威胁和风险，测试范围覆盖 Web 应用、操作系统、数据库、中间件、网络设备、API 接口、身份认证与权限控制及业务逻辑等各个层面，重点排查敏感数据泄露、越权访问、SQL 注入、XSS 跨站脚本、CSRF 跨站请求伪造、文件上传漏洞、命令执行等高危风险，对发现的漏洞进行利用验证和危害程度分析，并针对安全隐患提出解决办法，切实保证信息系统安全;加固后进行复测，检验安全加固效果。

供应商须提供适配采购人场景的自动化渗透测试解决方案，应具备自动化漏洞检测能力，以便快速识别系统潜在风险;需同时提供服务工具的功能界面截图，并加盖生产厂商公章作为技术能力证明。

服务频次：按采购人需求提供服务，服务期内不少于 4 次。

交付成果：《XX 系统渗透测试报告》（含漏洞详情、危害等级、影响范围、验证过程、整改建议等内容）。

5.2 上线前安全检查服务

供应商应对采购人提供拟上线的新模块、新功能进行上线前安全检测，根据系统上线要求开展基线核查、漏洞扫描、代码审计、开源组件检查、部署环境评估等安全检测，全面提升信息系统上线前的整体防护水平，保障信息系统上线后的整体安全性。针对发现的安全问题，给出整改建议并进行全程跟踪验证，确保所有高危及以上漏洞整改完成

后方可上线。

供应商须自带基线检查、漏洞扫描、代码审计、开源组件检测服务工具，使用检测工具需为自主研发，具备完整知识产权;禁止使用开源免费工具、社区版工具、二次开发改造工具或无资质第三方工具。

服务频次：按采购人需求提供服务，每次新增功能/系统上线前完成。

交付成果：《XX 系统上线前安全评估报告》、《上线安全评估意见书》（明确是否具备上线条件）

5.3 安全审计服务

供应商利用服务工具对信息系统、网络、数据、应用、管理制度及运维操作进行全面检查、合规校验、风险识别、行为追溯、闭环整改等，用于保障系统合规、数据安全、业务稳定，满足等保、数据安全法等监管要求，服务内容包括但不限于安全制度与合规性审计、网络与业务系统安全审计、数据安全审计、安全运维与管理审计等。

供应商须自带服务工具，服务工具需为自主研发，具备完整知识产权;禁止使用开源免费工具、社区版工具、二次开发改造工具或无资质第三方工具。

服务频次：按采购人需求提供服务，服务期内不少于 4 次。

交付成果：《XX 系统安全审计报告》、《合规性评估报告》、《风险清单与整改建议》

5.4 风险评估服务

供应商应采用定性与定量相结合的方法，对局属政务信息系统进行全面的安全风险评估，系统识别资产价值、威胁来源和脆弱点，科学分析安全事件发生的可能性和影响程度，准确计算风险等级并划分风险优先级;在安全管理体系评估中，不仅要评估安全策略、规章制度、程序、表单体系的完整性，而且会评估这些制度是否得到贯彻执行，是否及时更新，是否全面覆盖需进行信息安全风险评估的信息系统;在安全技术体系评估中，对信息系统面临的安全风险进行识别与分析，采用传统的风险评估方法，从资产、威胁、脆弱性的角度，对前端业务处理接口安全，业务数据传输安全、服务端的物理、网络、系统、应用、数据等层面的安全，进行风险值量化;制定包括风险规避、风险降低、风险转移和风险接受在内的风险处置方案，同时评估现有安全防护措施的有效性并提出针对性的安全加固建议。

供应商须按照《信息安全技术信息安全风险评估方法》（GB/T20984-2022） 国标标准对局属政务信息系统现有网络架构、安全设备、安全策略、业务系统访问控制等进

行详细的安全检查和测试评估，评估技术漏洞、管理漏洞及物理漏洞等，找出安全薄弱点，并协助整改。

服务频次：按采购人需求提供服务，服务期内不少于 1 次。

交付成果：《网络安全风险评估报告》、《数据安全风险评估报告》

5.5 安全漏洞复测服务

供应商应对所有采购人发现的漏洞进行整改后的复测验证，确认整改措施的有效性和漏洞的完全修复状态，对未完全修复或修复不彻底的漏洞提供进一步的整改建议，同时对整改过程中可能引入的新漏洞进行检测，建立并维护完整的漏洞整改闭环管理机制。

供应商须自带服务工具，服务工具需为自主研发，具备完整知识产权;禁止使用开源免费工具、社区版工具、二次开发改造工具或无资质第三方工具。

服务频次：按采购人需求提供服务，服务期内每个局属政务信息系统不少于 2 次

交付成果：《漏洞复测报告》（每次复测后提交）

5.6 专项安全检查服务

供应商应针对特定安全主题或重要时期开展专项安全检查，常规检查主题包括勒索病毒防护、重大活动保障检查、数据安全、移动应用安全、云平台安全、供应链安全及重大活动安全保障等，检查内容根据专项主题确定并重点排查该领域存在的突出安全问题，同时提供专项安全加固建议和针对性的应急处置预案。

供应商须提供全年的安全检查支持服务，包括现场检查、远程支持、问题复测等方面的服务。

服务频次：按采购人需求提供服务，服务期内不少于 2 次;突发安全事件立即开展针对性专项检查，不受服务频次限定。

交付成果：《XX 专项安全检查报告》

5.7 安全应急响应服务

供应商应根据所涉及的资产清单，结合局属政务信息系统部署环境，建立健全应急管理机制，编制完善应急预案，组织开展应急演练，验证预案有效性;梳理数据风险、网络攻击等场景处置流程;对于系统突发紧急故障，在接到通知后第一时间做出响应，开展专业的应急响应工作，并提交相应的问题处理方案、应急材料供采购人研判;故障处理完毕后出具故障分析报告，确保突发安全事件有效处置，保障业务连续性。

供应商须在接到采购人通知后 2 小时内采取相应措施以确保系统正常运行;无法在

2 小时内解决的，须在采购人要求时间内提交。

服务频次：按采购人需求提供服务，服务期内不限次数。

交付成果：《XX 系统网络和数据安全应急预案》

5.8 安全咨询服务

供应商应根据采购人需要，提供 7×24 小时电话和在线安全咨询服务，及时解答日常安全问题，协助制定和完善安全管理制度、应急预案及操作流程，提供安全事件应急响应咨询和技术支持，给出安全设备选型、部署和配置建议，持续跟踪国内外最新安全动态、漏洞信息和攻击手段并及时发布安全预警，同时协助开展等级保护测评、关键信息基础设施认定等合规性工作。

供应商须提供全年的安全检查支持服务，包括现场检查、远程支持、问题复测等方面的服务。

服务频次：按采购人需求提供服务，服务期内不限次数。

交付成果：安全服务月报（每月提供）、安全相关参考文件等。

5.9 网络安全风险威胁情报收集

供应商应根据采购人需要，采集多源异构威胁情报，包括但不限于 IP 信誉情报（支持 IPv4、IPv6，含威胁类型、严重级别、地理位置等标签）、IOC 失陷情报（支持 IP 及域名查询，可识别标注攻击团伙）、漏洞威胁情报（支持通过漏洞编号、名称等多维度查询）；同时整合开源情报、第三方商业情报及局属系统内部安全日志、网络流量等数据，确保情报来源全面、内容详实。对采集的原始情报进行清洗、去重、关联分析及人工研判，剔除无效、重复数据，确保情报准确性和可操作性。

每周向采购人提交一份标准化情报报告，明确威胁等级、影响范围、潜在风险及初步处置建议

服务频次：按采购人需求提供服务，服务期内不限次数。

交付成果：网络安全风险威胁情报报告。

6.驻场人员要求

供应商应提供不少于 6 人的驻场安全服务，其中项目经理、技术负责人、技术人员须符合技术配备相关要求。

驻场人员须工作日常驻采购人指定办公场地，提供 5x8 小时的现场安全服务，并通过电话、微信等多种方式，提供 7x24 小时的远程安全服务实现问题处置。

第七条 双方的权利与义务

7.1 甲方的权利和义务

7.1.1 甲方应当依据本合同的约定，向乙方支付监管服务价款。

7.1.2 甲方为乙方提供本合同项下所需要的资源，包括访问测评范围内网络设备和主机设备的权限及其他相关资料。

7.1.3 甲方确保乙方实施本合同项下的服务时，对于设备的使用、信息的获取和更改，不会违反任何保密或协议责任，不会侵犯第三方的权利。

7.1.4 甲方有权在乙方履行合同过程中出现损害或可能损害国家利益、公共利益、公共安全情形时变更、中止或者终止本合同。

7.1.5 甲方授权河南省政务大数据中心作为受委托方，负责项目服务过程中的技术性管理工作，具体包括：项目需求统筹，技术方案审核，项目安全保障和应急处置，对乙方提供的服务进行考核，对乙方服务质量进行监督，组织参与项目验收。

7.2 乙方的权利和义务

7.2.1 乙方应当按照甲方的要求，制定适用于本合同服务范围的内部质量和风险控制制度及措施，确保完成本项目的测评服务。

7.2.2 乙方人员在项目执行期间应保持相对稳定，以保证项目的顺利实施。乙方人员的变更需提前 3 日向甲方提出书面申请，并保证接替人员能够胜任此项测评工作，经甲方书面同意后方可变更，变更时做好该项目的技术及文档交接。参与项目的所有人员都应当受本合同各条款的约束。

7.2.3 乙方须确保乙方及项目组人员遵守附件 3《保密承诺书》的各项内容。

7.2.4 乙方在按合同要求实施测评的过程中，应当及时向甲方通报在信息系统中发现的安全问题，并协助甲方尽可能地弥补缺陷。

7.2.5 乙方应当接受并配合甲方组织的对本合同履行情况的监督与检查，对于甲方指出的问题，应及时作出合理解释或予以纠正。

7.2.6 乙方应当根据甲方要求，接受和配合甲方或甲方委托机构进行的与本合同相关的审计。

7.2.7 乙方在项目实施过程中出现资源、进度、质量协调控制不力的情况，甲方有权要求更换相关项目人员，乙方必须予以配合，并确保不影响项目的进度和质量。

7.2.8 乙方应当根据服务的内容和进度安排，按时提交阶段性技术报告及有关资料。

7.2.9 乙方在实施关键安全监管时（如漏洞扫描或工具测试等），要与甲方充分沟通该关安全监管实施的细节与步骤，得到甲方许可后，再开展该测评，以该测评项对甲方的信息系统影响最小化为目标。

7.2.10 项目交付后，乙方应当无条件返还甲方提供的文件、资料，同时乙方应当自留一份完整的项目档案按保密信息标准予以妥善保存，以便质保工作的顺利开展，但不得用于第三方和其他项目。

第八条 项目验收

8.1 乙方服务完成后，向甲方提交验收申请，由甲方组织项目的验收工作，乙方在合同期满前提交以下项目文档：

8.1.1 提交被测系统的《XX 系统渗透测试报告》；

8.1.2 提交被测系统的《XX 系统上线前安全评估报告》、《上线安全评估意见书》；

8.1.3 提交被测系统的《XX 系统安全审计报告》、《合规性评估报告》、《风险清单与整改建议》；

8.1.4 提交被测系统的《网络安全风险评估报告》、《数据安全风险评估报告》；

8.1.5 提交被测系统的《漏洞复测报告》；

8.1.6 提交被测系统的《XX 专项安全检查报告》

8.2 甲方收到以上文档后，组织人员开展验收。

8.3 验收完毕后，乙方应持续协助甲方开展整改工作，对整改后的成效按验收标准进行评审，重新出具测评报告。

第九条 合同价款、支付方式及履约保证

9.1 本项目合同总价款为人民币小写：￥_____元（含税价），人民币大写：_____元整（含税价）。

1. 首期款：签订合同后，乙方书面提交与拟支付金额等额的符合甲方财务管理要求的相应发票后_____个工作日内，启动首期款支付流程，支付合同总金额的20%，即人民币大写_____元整（￥_____ 元）。（如果支付款包含多项费用，应当按大类分别列出支出明细；如果支付的款项需要支付给不同的公司，要按公司分别支付，以下同。）

2. 进度款：截至_____年____月_____日，结合对前期绩效评估结果，已具备进度款支付条件。甲方在收到乙方书面提交支付申请函及与拟支付金额等额的符合甲方财务管理要求的相应发票后_____个工作日内，启动进度款支付流程，支付合同总

金额的30%，即人民币大写：_____元整。（￥_____元）。

3.尾款：合同履行期满，经甲方确认验收合格后，依据绩效评估结果计算金额扣除已支付金额以及违约金额计算支付，甲方在收到乙方书面提交支付申请函及拟支付金额等额的符合甲方财务管理要求的相应发票后_____个工作日内，启动尾款支付流程，即人民币大写_____元整（￥_____元）。

9.2 乙方在甲方支付合同款项前，应先按各期付款数额在10个工作日内向甲方开具符合国家法律法规和标准的税务发票，之后甲方按程序向乙方进行支付。若乙方未提供合法有效的发票，甲方有权拒付款项，且不承担违约责任。

第十条 合同变更

10.1 如本合同在履行过程中有任何变更、补充或修改，都必须经甲乙双方协商同意，必要时依据重要程度由双方法定代表人或授权代表另行签订书面协议。

10.2 甲方提出变更要求

10.2.1 如甲方要求变更项目服务内容，应当以书面形式将相关要求提交给乙方。乙方应当在7个工作日内，对该变更后在项目交付日期、工作量、影响范围等方面做出评估，并书面回复甲方。

10.2.2 甲方在收到乙方回复后，应当在7个工作日内，以书面方式通知乙方，对是否接受进行回复。因甲方提出的变更导致工作量增加的，如果增加的工作量不超过总量的20%，则合同总价不作调增；因甲方提出的变更导致工作量减少的，如果减少工作量不超过总量的20%（含），则合同总价不作调减。如果增加工作量超过总量的20%，甲方将视增加的服务为新项目，另行立项。如果减少工作量超过总量的20%，经双方共同协商后，签订补充协议，按比例调整合同总价。

10.2.3 合同履行期间甲方因业务职能或重大政策发生变更或因其他原因导致合同无法继续履行时，甲方有权解除本合同，且不承担任何违约责任。合同未履行部分的费用不再支付，已支付部分按未实施的服务部分比例或剩余服务时间的比例进行返还，未支付部分按已实施的服务部分时长与全年时长比例进行支付。

10.3 乙方提出变更建议

10.3.1 如乙方要求变更项目服务内容，乙方应当对该变更后在项目交付日期、工作量、影响范围等方面做出评估，并以书面形式提交给甲方。

10.3.2 甲方在收到乙方的变更建议后，应当在7个工作日内，以书面方式通知乙方是否接受乙方的变更建议。如甲方接受乙方的变更建议，因乙方提出的变更导致工作量

增加的，则合同总价不作调增；因乙方提出的变更导致工作量减少的，如果减少工作量不超过总量的 20%（含），则合同总价不作调减。如果减少工作量超过总量的 20%，则经双方共同协商后，签订补充协议，按比例调整合同总价。

第十一条 知识产权

11.1 乙方在履行和完成本合同项下工作过程中准备及形成的一切资料，包括但不限于文件、计算方法、图表、报告、数据、模型和样品，以及其中含有的所有发明为甲方所有，甲方有权使用上述资料以履行本项目合同或用于其他目的。该资料应与本项目合同项下其他资料一起，按要求在本项目合同结束或终止的时候，交还给甲方。

11.2 本项目所形成的产品其知识产权归甲方所有，乙方非经甲方书面同意，不得以任何方式向第三方披露或转让。除本项目测评需要外，乙方不得以任何方式在任何情形下利用。

11.3 涉及乙方的测试流程、测试方法、分析方法、方案模板、报告模板等相近知识产权内容归乙方所有。

第十二条 保密

乙方须与甲方签订保密承诺书作为合同附件，见附件 3。

第十三条 违约责任及损失赔偿

13.1 如果乙方在工作中发生重大及以上安全事件，包括但不限于由于乙方故意或过失等原因造成甲方系统出现重大网络中断、数据丢失、系统瘫痪或者出现反动言论等情况，甲方有权决定是否解除合同，乙方须承担由此给甲方带来的一切损失。

13.2 乙方违反合同约定的保密义务，乙方应当支付合同总价 1%的违约金。如实际损失超过违约金的，甲方有权要求对方赔偿超过部分。

13.3 任何一方违反合同约定的知识产权保护条款，除立即停止违约行为外，还应当支付合同价款的 1%作为违约金。

13.4 乙方工作人员未经甲方授权，擅自篡改甲方业务数据，或利用甲方现有业务信息系统、网络平台或者冒用甲方身份获取非法利益，造成甲方或任何第三方损失的，由乙方承担法律责任并负责赔偿全部损失，同时乙方须向甲方支付本合同总价款 1%的违约金。

13.5 因乙方原因造成严重超期、拖延而不能按时交付，自交付日期起，每超期一周乙方应当支付合同总价 1%的违约金。

13.6 如乙方工作人员擅自承担或参与涉及甲方职能的行政业务工作，对甲方造成

不良影响的，乙方应立即停止其行为并采取发布声明等措施消除影响，同时甲方保留追究乙方法律责任的权利。

13.7 如乙方发生违约事件，甲方要求乙方支付违约金或赔偿款时，应当以书面方式通知乙方，内容包括违约事件、违约金、支付时间和方式等。乙方在收到上述通知后，应当于 7 日内答复甲方，并支付违约金或赔偿金。逾期未支付的，甲方有权在合同款项中予以扣除。

13.8 服务期限内，如乙方发生违约事件累计超过三次，甲方有权单方终止合同，并将乙方列入不良行为记录，甲方有权限制乙方参与甲方此后的测评服务项目。

第十四条 不可抗力

14.1 本合同中不可抗力系指甲乙双方在缔结合同时所不能预见的、并且它的发生及其后果是无法避免和无法克服的客观情况。

14.2 由于不可抗力致使合同无法履行的，受不可抗力影响一方应立即将不能履行本合同的事实书面通知对方，并协助对方最大可能减少损失，在不可抗力发生之日起 7 日内提供有关政府部门或公证机关出具的证明文件。

14.3 本合同在不可抗力影响范围及其持续期间内将中止履行，本合同执行时间可根据中止的时间相应顺延，双方无需承担违约责任。不可抗力事件消除后，双方应当就合同的履行及后续问题进行协商。

第十五条 合同转让及终止

15.1 合同转让：非经双方书面同意，任何一方无权转让本合同及该合同约定的全部或部分权利、义务。非经对方同意擅自转让的，对方有权解除合同，并要求擅自转让方承担全部赔偿责任。

15.2 合同终止

15.2.1 合同自然终止：甲乙双方全部履行合同约定的义务后，本合同自然终止。

15.2.2 违约合同终止：若合同一方有足够证据证明合同另一方未在规定时间内履行本合同项下规定义务，可向对方提出书面违约通知，提出终止部分或全部合同，合同中未终止的部分应继续履行。

15.2.3 无能力履行合同终止：如有充分证据证明乙方无清偿能力或无继续履行合同的能力，甲方可以在任何时候以书面形式通知对方，提出终止合同而不给对方补偿，或要求资产保全防止损失扩大。

15.3 双方协商一致可以终止合同。

第十六条　适用法律及争议解决

16.1 本合同按中华人民共和国法律解释。

16.2 甲、乙双方在合同履行过程中发生的一切争议，均应通过双方友好协商解决；协商不成的，任何一方均可向甲方住所地人民法院提起诉讼。

16.3 在诉讼期间，除正在进行诉讼的部分外，本合同的其他部分应当继续执行。

第十七条 合同的生效

17.1 本合同经双方盖章以及法定代表人或授权代表签字后生效。

17.2 本合同一经签署，未经双方书面同意，任何一方不得随意更改。

17.3 本合同一式肆份，甲乙双方各执贰份，具有同等法律效力。

第十八条 其他

18.1 如一方改变通讯地址及其他信息，应当在变更后 7 日内以书面方式通知另一方，否则，由此而造成的损失，由信息发生变更的一方承担。

18.2 本合同未尽事宜，双方可以另行协商签订补充协议，补充协议经双方盖章以及法定代表人或授权代表签字后与本合同具有同等效力。

（以下无正文，仅为签章页）

甲方（盖章）：_____

法定代表人或授权代表（签字）：_____

统一社会信用代码：_____

联系人：_____

联系电话：_____

地址：_____

2026 年　月　日

乙方（盖章）：_____

法定代表人或授权代表（签字）：_____

统一社会信用代码:_____

开户银行及账号：_____

联系人：_____

联系电话：_____

地址：_____

2026 年　月　日

附件 1-1

项目人员名单

职务	姓名	职称	执业或职业资格证明				备注
			证书名称	级别	证号	专业	

附件 1-2

绩效考核标准

序号	评价指标	评分内容	分值
1	服务交付及时性	按合同及甲方要求，按时完成渗透测试、安全检查、风险评估、安全审计等服务报告编制并交付。未按时交付或成果不满足要求，每次扣 1 分，扣完为止。	10 分
2	人员管理	保障项目服务团队稳定，未经甲方同意不得随意更换现场服务人员，违规每次扣 1 分；服务人员专业能力、资质不符合项目要求，每次扣 5 分，扣完为止。	10 分
3	服务质量	安全检测、审计、评估、复测、专项检查等工作成果符合国家网络安全标准及甲方要求，交付成果不达标每次扣 2 分。	10 分
4	响应及时性	工作时间：在合同约定的工作时段内，必须确保电话畅通，及时接听甲方人员电话通知 5 分钟内响应,否则视为非及时响应，每发生一起非及时响应扣 3 分； 非工作时间：在非工作时段，应确保 24 小时电话开机。在需要紧急服务支撑时，在接到甲方人员通知后 30 分钟内赶到现场视为及时，否则视为非及时响应。每发生一起非及时响应扣 2 分。	14 分
5	常态化渗透测试	按计划完成常态化渗透测试，未按频次开展、重大风险隐患未识别，每次扣 2 分。	7 分
6	上线安全检查	新增功能/系统上线前按要求完成安全检查并出具报告，未执行或检查不到位导致上线风险，每次扣 2 分。	7 分
7	安全审计服务	按计划完成常态化安全审计、日志审计、行为审计，按时提交审计报告，未按要求开展、审计漏项、重大风险隐患未识别、报告不合格或未及时提交，每次扣 2 分，扣完为止。	7 分
8	风险评估	按计划完成全流程风险评估，识别系统安全风险并形成评估报告；未按计划开展、风险漏判、报告不合格、未按时提交，每次扣 2 分，扣完为止。	7 分

9	安全漏洞复测	对漏洞按期完成复测，跟踪整改闭环，未复测或未跟踪导致风险长期存在，每次扣 2 分。	5 分
10	专项安全检查	按要求针对勒索病毒防护、重大活动保障、数据安全、移动应用安全、云平台安全、供应链安全等主题开展专项安全检查，并提供专项安全加固建议与针对性应急处置预案。未开展、检查不全面、未提供加固建议或预案、报告不合格，每次扣 2 分。	6 分
11	安全应急响应服务	建立应急管理机制、编制应急预案、组织应急演练；梳理数据风险、网络攻击等处置流程；接到通知后 2 小时内采取措施保障系统运行，及时提交处理方案与应急材料，故障处理后出具分析报告。未落实、响应超时、处置不当、未提交材料，每次扣 3 分。	6 分
12	安全咨询	按要求提供安全咨询解答、协助制定和完善安全管理制度；未响应咨询、支撑不到位，每次扣 2 分。	5 分
13	网络安全威胁情报收集	按要求定期收集、研判、报送网络安全风险威胁情报，未按频次收集、漏报重要情报、未及时预警，每次扣 1 分。	3 分
14	过程文档	按进度提交过程文档、检测记录、处置台账，未按时提交、内容不完整，每次扣 1 分。	3 分
15	否决项	因渗透测试、安全检查等操作不规范导致系统瘫痪；因重大风险隐患未识别引发网络安全事件；利用工作便利植入恶意病毒、设置后门程序、盗取数据等。	出现一次重大及以上安全事件，甲方有权终止合同。
合计			100 分

服务款项结算标准

序号	评价分数范围	评价等级	支付比例
1	90 分≤评价≤100 分	优秀	100%
2	75 分≤评价<90 分	良	90%
3	60 分≤评价<75 分	中等	70%
4	评价低于 60 分	不合格	50%

备注：

1．服务结算标准是依据服务质量评价结果确定的服务费的支付比例。

2．上述结算标准仅作为甲方对乙方的服务质量评价结算标准，不作为验收条件。

3．计算公式：服务金额=合同总金额*评价分数对应的支付比例。

附件 1-3

廉洁承诺书

为加强商务活动中的廉政建设，防止发生各种谋取不正当利益的违法违纪行为、规范合同双方的各项活动，保障顺畅、公平的商业秩序，保护当事人的合法权益，根据《中华人民共和国民法典》等相关法律，我司承诺以下廉政责任：

一、我司承诺在与甲方的商务往来活动中遵循自愿、公平、等价有偿、诚实信用原则，并保证在合同订立、履行过程中以及事前事后保持公开、公平、公正、诚信、透明的原则，不会为获取不正当的利益，损害国家、集体和甲方利益。

二、我司保证我司以及我司工作人员与甲方保持正常的业务交往，按照有关法律法规的规定和程序开展业务活动，并遵守以下规定：

（一）不以任何理由向甲方工作人员提供或赠送礼金、有价证券、贵重物品及回扣、好处费、感谢费等。

（二）不以任何理由为甲方工作人员报销应由甲方工作人员个人支付的费用。

（三）不接受或暗示为甲方工作人员在装修住房、婚丧嫁娶、配偶子女的工作安排以及出国（境）、旅游等方面提供便利。

（四）不为甲方工作人员提供通信工具、交通工具和高档办公用品等物资。

（五）不以任何理由为甲方工作人员组织有可能影响廉洁、公正的宴请、健身、娱乐活动。

（六）不许诺事后给予甲方工作人员利益。

（七）不以其他手段为甲方工作人员提供其他不正当利益。

（八）上述条款中所称不正当利益包括但不限于金钱和实物。如回扣、佣金、股份、股东资格、债券、促销费、赞助费、广告宣传费、劳务费、红包、礼金、含有金额的会员卡、代币卡（券）、旅游费用、就业机会、项目机会、各种高档生活用品、奢侈消费品、工艺品、收藏品、房屋、车辆、减免债务、提供担保、免费娱乐、旅游、考察、提供房屋装修、借贷款项、借用物品、特殊待遇等财产性或者非财产性利益等。

三、我司同意，如违反以上约定，甲方有权终止合同，相关的责任由我司承担；涉嫌犯罪的，甲方有权移交司法机关，并追究刑事责任。若因此给甲方造成经济损失的，我司同意按有关规定予以赔偿。

承诺方（盖章）：_____

签字日期：____年___月___日

附件 1-4

保密承诺书

根据《中华人民共和国保守国家秘密法》及有关规定，为保护项目涉及的工作或敏感信息，在遵循平等自愿、诚实信用的原则下，经协商一致，乙方就在履行本项目合同义务期间（以下简称“项目”）的保密事项，签订本承诺书，接受本承诺书的约束。

一、保密范围和内容

乙方通过参与甲方项目知晓的，以及在项目实施过程中产生的国家秘密、工作秘密或内部、敏感的信息和数据，包括但不限于：

（一）商业信息

1.承诺方在项目实施过程中了解的甲方单位性质、人员信息、工作内容、机构设置、责任分工、联系方式等信息；

2.承诺方知晓的甲方与其他公司的洽谈、合作、约定、协议、合同等信息。

（二）项目信息

1.项目相关应用系统业务需求、设计和实施方案、图纸、施工文档、测试报告、业务系统数据等信息；

2.甲方在项目实施过程中签署的会议纪要、谈判记录、招投标文件、合同书、变更、补充协议、往来函件等其他信息；

3.甲方设备安装场地、基础设施、机房、网络拓扑结构及其相关资料；

4.所涉及甲方信息系统的对接、漏洞、接口等信息；

5.甲方安全机制、安全系统，备份策略、应急演练及应急预案等；

6.项目其他相关文件、资料、技术文档、声像资料等。

（三）数据信息

1.项目相关设备数量、型号、配置、安装地点、运行状况等信息；

2.项目实施相关软件需求、设计文件、软件架构、源代码和可执行代码、程序文档、数据库、数据备份等资料；

3.项目实施所产生的所有数据（包括原始数据、过程数据、结果数据、日志数据、运维过程中产生的数据或信息等）及数据应用；

4.承诺方为甲方实施项目而通过其他渠道获取的与项目有关的数据信息；

5.其他经甲方确定或法律规定为国家秘密、工作秘密或内部、敏感的信息的所有事项。

二、乙方及其工作人员保密义务

乙方及其工作人员只能为项目工作目的使用甲方的项目资料，且仅限于项目管理人员及直接参与项目工作的人员知悉，不得扩大知悉范围、泄露给任何第三方或作与项目无关的使用。在项目实施过程中，承诺方及其工作人员应当遵守甲方关于项目人员、项目信息载体、项目场所与设备、项目管理等相关规定，包括但不限于：

1.乙方应当对承诺约定的保密文档妥善保管，并对参与项目的人员及其分工作出详细文字记录，由项目保密员统一管理。

2.乙方需要与其他单位合作完成项目的，应征得甲方书面同意，并保证合作单位具有相应资质。

3.乙方应当与参与项目的人员分别签订一份保密承诺，该承诺的实质内容应当与本承诺内容相一致，未签署保密承诺的人员不得参与项目。

4.乙方应当对参与项目人员进行有效地管理。定期进行保密教育、培训和保密自查，及时发现和纠正项目保密工作的偏差，对违反保密规定的人员及时处理，并通报甲方。乙方参与项目的人员在项目实施过程中离职的，乙方应当立即将该情况通知甲方，并要求离职人员清理和移交本人保管的资料、文件、数据等含有项目信息的载体，离职人员需继续遵守该保密承诺。

5.乙方项目实施场地必须满足项目实施要求，实行严格的管理制度。在甲方场所内办公的，遵守甲方管理要求，不得接触与项目无关的信息，不得获取和掌握甲方各系统的用户名和密码，对于项目相关数据、信息未经允许不得私自存储、拷贝、复印、带离等。

6.乙方不得泄露甲方与乙方或与其他任何第三方的谈判合作信息等商业信息。

7.禁止将与项目有关的信息上传到互联网网站、论坛、网盘和社交媒体等，确需由邮件形式发送的必须加密处理。

8.项目的设计方案、研发成果及有关建设情况，不得擅自以任何形式公开发表、交流或转让、申请专利或申报国家奖励。

9.未经甲方书面许可，乙方不得使用甲方案例用于宣传、投标、技术交流等。

10.未经甲方书面许可，乙方不得留存甲方任何数据信息，不得以任何方式私自对项目有关数据的任何版本进行分析、加工、处理，不得以任何形式提供给其他第三方。

11.乙方不得泄露包括专利技术、技术秘密、产品信息、客户信息等甲方任何无形资产。

12.对于乙方在本承诺生效之前或承诺终止后,通过保密承诺任何途径知悉或取得的有关甲方的重要信息，在本承诺生效后，乙方应当参照承诺履行相应的保密义务。

13.乙方在本承诺中承担的保密义务，不因本项目的中止或终止而解除。

14.乙方所邀请的第三方专业测试人员、技术支撑人员、相关厂商支持等外援人员，将严格按照项目相关要求开展项目工作，未经甲方书面同意，绝不随意传播项目信息。技术支持工作结束后，乙方需严格监督其妥善移交相关文件资料，绝不擅自销毁或另作他用。如因第三方人员问题产生的信息泄露，由乙方承担主要责任。

15.如因乙方技术、管理等原因，发生数据泄露、损坏、遗失，乙方必须承担相应赔偿等责任。

三、人员登记制度

乙方所有参与项目的人员应当保证履行本承诺约定的各项义务，如实填写“项目人员名单”，且每页加盖单位公章方为有效。乙方对其工作人员登记信息的真实性负责。在项目实施过程中增加的人员，乙方应当在人员入场前追加填写“项目人员名单”。原厂实施人员，应当同时加盖原厂单位公章和乙方公章方为有效。乙方应当按照国家相关保密管理规定，严格禁止除登记人员以外的人员知悉项目的一切信息。乙方应当对参与政府信息化建设的关键数据岗位人员开展必要的安全背景审查，确保数据安全。

四、工作联系

为落实好本承诺，乙方应当采取必要的措施防止任何泄密情况的发生，并指定专人负责双方之间的保密工作关系，并随时就本承诺的保密事宜进行研究和落实，乙方特选派_____为专项联系人。

五、通知

乙方发现有失密、泄密、窃密等行为发生的，应当立即通知甲方，并应当密切协作，尽快查明事件原因、过程、后果等情况。

六、保密期限

乙方的保密义务为无限期保密，即从本承诺签订之日起承担保密义务。

七、争议解决

本承诺条款，如存在与国家有关法规相抵触，按照国家有关法规执行，双方若发生争议，应当首先友好协商解决，协商不成，任何一方均可向甲方住所地人民法院提起诉

讼。

八、其他要求

1.双方就项目所签订的合同变更、解除或提前终止的，本承诺效力不受影响。

2.未经甲方和乙方双方事先书面达成一致意见，本承诺书不得以任何其他理由而更改。

承诺方（盖章）:_____

签字日期：_____年____月____日

第五章 采购需求

河南省行政审批和政务信息管理局2026年度局属政务信息系统运维项目采购需求

A包:局属6个政务信息系统综合运维项目采购需求

A包：河南省省级一体化政务服务平台（一期）（除电子证照系统）采购需求

河南省省级一体化政务服务平台运维工作应对业务系统、信息资产和安全资产进行全面梳理，形成《系统及功能清单》《系统资产清单》和《安全资产清单》，以资产清单为依托，重点开展河南省一体化政务服务平台的统一用户管理及认证平台、网上政务服务门户、政务服务事项管理系统、政务服务运行管理系统、政务服务办件信息系统、电子监察等系统和政务数据共享门户服务平台等系统运维工作，提供符合运维工作有关规定的系统优化升级、数据加工等服务，通过开发或者采购提供稳定、安全、可靠的短信发送、用户信息核验、实人刷脸控件等服务，配合开展网络安全等级保护测评工作，开展安全运维工作。具体运维需求如下：

1.基础环境及软件运维

根据实际运维工作需要，对平台的主机、数据库、中间件和业务系统的运行状态和性能指标进行监控，对运行日志进行采集和存储，并可提供日志查询和统计分析。主要运维要求：保障平台7×24小时不间断运行，针对基础环境运维保障系统总体可用率不低于99.9%，日志保存时间不低于一年，运维期内无重大故障发生，无重大安全事故发生。

1.1服务器运维内容

服务器日常运维。对新下发的服务器完成操作系统初始化、操作系统优化、操作系统安全加固、接入运维管理工具和日志采集平台等工作；对下发的漏洞扫描结果在规定时间内完成服务器漏洞修复，保障高危漏洞3日内完成修复，中危漏洞7日内完成修复，漏洞修复较复杂的应在3日内制定详尽的漏洞修复方案，报送采购人审批通过后，按照方案执行。

服务器运行监控。对服务器运行状态进行日常监测、对预警问题按照问题处理规范进行问题记录、流转、处理和跟踪等工作，建立健全的系统问题处理机制和规范，保障

主机长期处于最优状态。在采购人界定的问题程度下，一般问题 2 个小时解决并记录，较严重问题 4 个小时出具问题解决方案并提交给采购人研判解决。

服务器资源全生命周期管理。对现有资源进行全面梳理，全面管理资源的申请、调整、释放工作。

1.2 中间件运维内容

中间件安装和漏洞修复。根据实际工作要求完成所需中间件的安装、集群搭建、优化、配置、调试和安全加固等工作，开展问题定位排查处理。在采购人界定的问题分类下，一般问题 2 小时内解决，较严重问题 4 小时内出具问题解决方案并提交给采购人研判解决。

中间件运行监控。每日开展中间件的系统监控和问题处理工作，保障中间件长期处于最优状态。

1.3 数据库运维内容

数据库安装和漏洞修复。根据实际工作要求完成常用数据库部署、集群的搭建、配置和优化工作；数据库漏洞应在 2 日内编写详细的漏洞修复方案，提报给采购人研判，并按要求完成数据库安全加固和整改，保障数据库的稳定运行。

数据库运行监控。针对数据库运行状态进行全面监测，监控指标包括数据库运行指标、集群监控指标、表空间使用情况、慢 SQL 指标，对发现的问题应在 2 小时内进行定位并协调相关方处理，保障数据库长期处于最优状态。

数据库备份恢复和扩容。按照备份管理要求，对数据库进行备份和巡检。

1.4 日常巡检要求内容

提供每日不低于 1 次的操作系统、中间件、数据库、业务系统等运行指标、应用进程运行情况巡检工作，对预警和发现的问题和隐患，提出处理建议或修复方案，并及时处理，一般问题 2 个小时解决，较严重问题协调相关人员 4 个小时出具问题解决方案并提交给采购人研判解决。做好系统资源监控，按政务云要求优化系统资源使用，需进行配置变更时，提供资源变更申请，做好系统资源变更后运行监控。

1.5 运行情况报告内容

月度运维报告。根据业务系统业务办理情况，关键核心业务接口、数据接口调用量，用户量、注册用户数、访问人数，基础环境等运行情况及异常信息，出具业务系统运行报告；对运维工作进行梳理，出具运维月报；根据系统监控数据，对服务器的负载综合分析，出具服务器负载报告；根据数据库运行监控数据，组织数据库运维人员对数据库

进行全面检查和综合评估，按月出具数据库健康状态报告，包括数据库部署运行情况、数据库备份情况，慢 SQL 数据情况、数据库优化建议。

季度运维报告。每季度进行系统运行和运维工作总结，提交季度系统运行工作报告，内容包括本季度内的系统运行情况，运维工作情况，需求完成情况，故障及处理情况，安全工作开展情况，其他需要汇报或讨论的内容及下个季度的工作计划等。

年度汇报。每年度进行系统运行和运维工作总结，提交年度系统运行工作报告，内容包括本年内的系统运行情况，运维工作情况，故障处理情况，安全工作开展情况，其他需要汇报或讨论的内容及下个周期工作计划等。

1.6 网络软硬件维保服务

对安全设备的安全识别库、入侵特征库、病毒检测特征库等升级服务、定期设备巡检、故障处理修复、版本升级、设备保修服务。

2.业务系统运维

根据对河南省省级一体化政务服务平台业务流程、数据处理流程、信息更新流程等理解程度，形成《业务系统及信息资源维护方案》。主要包括包含：1、统一用户管理及认证平台；2、网上政务服务平台门户；3、事项中心；4、政务服务运行管理系统；5、政务服务办件信息系统；6、电子监察系统；7、政务数据共享门户服务平台；系统、数据库、中间件、系统运行等保障系统正常运行等基础运维要求均适用于以下系统，不再逐一表述。

2.1 统一用户管理及认证平台

运维范围包括但不限于用户管理、权限管理、配置管理、注册管理、认证管理、对接管理功能模块的业务维护与配置，故障处理，漏洞修复，性能优化等工作。按照采购人要求完成业务影响分析、沟通汇报及回归测试、值班值守、节假日及特殊活动重保、数据信息核查与修改、数据解密、数据补全和数据推送、数据备份等。制定已接入业务系统动态管理清单，分部门分地市进行管理，包括新增接入系统、已接入系统域名调整、已接入系统重新对接、已接入系统停用、不满足安全要求清理的系统等日常管理。依据《河南省一体化政务服务平台统一身份认证系统接入管理办法（试行）》相关安全要求，定期核查已接入业务系统提供的安全资料完备性，梳理不满足《办法》中有关安全要求的系统明细清单（清单中需明确不满足哪些安全要求）及时报送采购人。

2.2 网上政务服务门户

运维范围包括但不限于开展分厅站点信息、公示公告、弹窗、阳光政务、热门服务、

特色服务、老年人服务专区、便民服务专区数据更新，维护事项、服务、适老化组件、网站公共组件相关参数；按采购人要求提供统计分析、咨询投诉处理、网站上线板块内容和服务的监测和问题处理、应用服务升级改造和功能验证；按照每日、每月、每季度、每半年统计政务服务网的页面访问情况、用户活跃数情况，同比、环比趋势分析以及用户访问激增时段的情况分析等。

按照国家平台质检要求优化政务服务“好差评”数据入库规则，及时向国家平台推送政务服务“好差评”数据；按照采购人要求配置政务服务“好差评”功能、优化评价页面、处置故障，解答和处理省市统一受理系统、省垂建业务系统与政务服务“好差评”对接中的问题，开展统计分析模块配置优化、评价数据整理、差评申诉确认等工作。

2.3 事项中心

运维范围包括但不限于按照国家质检要求定期向国家平台推送事项信息，处理事项质检过程中发现的异常数据，并对导致异常数据的系统功能进行及时修复；保障事项中心正常运行，按要求向省直相关部门和各省辖市（含济源示范区、航空港区）及时、准确、全量推送事项数据，确保“事项同源”，解决公众侧和政务侧反馈问题；提供政务服务事项（含便民服务应用、中介服务事项、跨城通办事项等）梳理与维护、基本目录管理、实施清单管理、事项要素模板管理、业务办理项管理、事项发布流程配置、事项接口标准制定与发布、事项数据统计分析、定期开展政务服务事项及其办事指南覆盖度、完备度和规范性巡检等服务。

2.4 通用审批系统

运维范围包括但不限于提供事项配置、组织机构配置、人员配置、业务流程配置、共享数据和材料配置、审批结果与电子证照关联配置等服务，强化数据共享在审批过程中的运用，根据审批部门业务办理需要，与国家部委或省级相关部门业务系统开展数据对接，及时解决运行过程中审批部门反馈问题和办件异常数据。按需开展办件数据修复，事项配置、组织机构配置、人员配置、业务流程配置、共享数据和材料配置、审批结果与电子证照关联配置，应用、数据库问题修复，供应商需要对维护内容、频次、数据范围、方式进行描述。

2.5 政务服务办件信息系统

运维范围包括但不限于按照国家质检要求定期向国家平台推送办件信息，处理质检过程中发现的异常数据，并对导致异常数据的系统功能进行及时修复；按需开展新的办件数据汇聚对接任务；持续做好办件汇总管理、办件分析、办件查询等模块的业务维护

和配置、故障处理。按照采购人要求完成办件数据汇聚过程中遇到的问题排查和处置、质检规则优化、异常数据修复、办件数据删除、办件数据处理、办件数据分发等工作。收集办件汇聚过程中各地各部门和企业群众反馈的共性、突出问题，持续优化办件对接标准规范。制定并持续完善办件测试流程技术指导规范，严格规范测试办件的生成标准、时限要求、清理流程、测试办件产生部门确认等。

2.6 电子监察系统

运维范围包括但不限于完善电子监察规则、调整电子监察范围和处理工作推进过程中遇到的问题，开展监察事件处理、监察规则优化、基础信息配置、故障处理等工作。做好统计分析模块的业务维护和配置，按照采购人要求完成解答和处理省直单位和省辖市在监察过程中遇到的问题、申诉数据核实、监察数据整理、监察数据处理工作。

2.7 政务数据共享门户服务平台

运维范围包括但不限于确保平台现有库表、文件夹交换和接口对接等数据共享任务的平稳运行，开展数据共享任务向省大数据平台迁移过程中的技术支撑工作。

信息资源维护内容包括：包括但不限于保障服务器、数据库、应用等平稳运行，确保日志服务正常，做好省行政审批政务信息管理局和其他省直部门、省辖市业务系统的政务数据目录迁移技术支撑工作。供应商需要对维护内容、频次、数据范围、方式进行描述。

3.政务服务工单运维

做好 12345 便民热线关于一体化政务服务平台及移动端日常工单处置办理，做好政府网站纠错反馈问题的，按期办理相关事项，规定时间内反馈工作处置结果，形成工作闭环。

4.短信服务运维

4.1 短信服务费用

支撑河南省省级一体化政务服务平台和河南省一体化协同办公平台两个系统的短信服务费用。2026 年预计短信发送 3000 万条（以实际使用量为准），服务期以合同为准。单价不超过 0.04 元/条。

4.2 短信服务平台能力需求

支持河南省省级一体化政务服务平台各业务子系统短信发送能力，包括但不限于以下方面的能力：

（1）具备并实现短信群发，包括但不限于短信平台页面、接口以及 APP 等，具备在

发送至全国范围的中国移动、中国联通、中国电信、中国广电以及虚拟运营商手机用户、携号转网手机用户的信息上下行送达能力，并支持实时返回短信的发送状态。

（2）具备并实现短信存储转发，支持短信持久化存储。

（3）具备并实现错误重发机制，避免网络原因造成短信发送失败。

（4）具备并实现流量控制，确保短信有序、全量发送。

（5）具备并实现丰富的鉴权功能，确保信息安全。

（6）具备并实现丰富的查询、统计分析功能。

（7）具备并实现短信签名，符合通信管理部门有关要求。

（8）具备并实现长短信发送，支持发送长短信功能，最多可达 300 个字。

（9）具备并实现模板导入与定时短信，针对不同用户发送不同内容,支持批量发送，可以实现短信定时自动发送。

（10）具备并实现发短信状态查询，在发件箱中可以查询到已发送的短信内容、号码、接收状态等，在收件箱中能够查看上行发送的短信，对于发送失败的短信，返回状态报告。

（11）具备并实现关键字过滤，支持设定关键字过滤库机制，短信内容中有匹配关键字过滤的内容该短信不予以发送，并有拦截的回执。

（12）具备并实现黑/白名单管理功能。

（13）与相关运营商建立对接沟通机制，及时排查处置企业群众反映的短信发送和接收方面存在的问题。

5.扫脸控件运维

包括扫脸控件和活体检测拓展服务。

供应商需根据国家关于用户办理事项时需进行实人核验的要求，提供集成扫脸控件功能，提供实人核验的软件支撑。扫脸控件须提供端侧活体检测功能，活体检测需符合国家的安全要求，控件产品需通过国家网络与信息系统安全产品质量监督检验中心检测。

单图活体检测拓展内容：支持针对输入的图像进行活体检测，可以抵御呈现式攻击：包括二维照片，屏幕，3D 头模，面具等的检测攻击检测。支持针对活化、贴图、AI 换脸等深度伪造的图像的检测分析。

6.用户信息核验

用户信息核验服务包括：

（1）对接国家网络身份认证公共服务平台，具备通过网络身份认证公共服务平台，为自然人提供申领网号、网证以及进行身份核验等网络身份认证公共服务的能力。

（2）四要素实名信息核验。开展用户四要素补齐并定期（每半年）检查用户信息变化。

（3）四要素实人信息核验。主要用于用户注册、用户信息补全和需实人核验（刷脸）办理业务。省一体化政务服务平台门户（政务服务网、“豫事办”、自助终端）上线登录补齐四要素和用户信息补全功能，上线一批“高效办成一件事”等需要实人核验业务。

（4）并发性能扩展。满足已接入系统、应用服务实人核验需求。

（5）符合其满足国家相关网络安全、数据安全法规要求，针对管理部门提出的监管要求和安全风险，应在要求期限内进行修复。

7.证书服务

（1）根据业务或需要，购买或提供企业级通配型 SSL 证书，包含企业级国际版（支持 RSA 或 ECC 算法）证书和国密版（国密 SM2 算法）证书。

（2）根据业务或需要，采购或提供单域名国际版（支持 RSA 或 ECC 算法）证书，支持常用浏览器及终端访问。

（3）根据河南政务服务网的服务范围及规模，采购或提供企业版 DNS 云解析服务。

8.数据分类分级

参照《数据安全技术 数据分类分级规则》（GB/T43697—2024）《全国一体化政务大数据体系 政务数据目录 第 3 部分：政务数据分类》（征求意见稿）和河南省一体化政务大数据体系工程标准《政务数据 分类分级指南》完成系统生成数据的分类分级梳理工作，系统汇聚的数据按照行业上级业务指导部门制定的数据分类分级要求开展数据分类分级工作。

9.安全运维

9.1 日常安全监测

组织专业技术力量，依托省级数字政府“一道墙”安全运营支撑平台、电子政务外网态势感知平台和自身监测能力，对河南省省级一体化政务服务平台（一期）（除电子证照系统）系统进行 7×24 小时监测，分析研判系统面临的网络安全攻击，对可能发生的网络安全、数据安全隐患进行处置，确保系统安全稳定运行。

9.2 安全漏洞修复

及时修复网络安全管理、保密管理、密码管理、公安、电子政务、行政审批和政务信息管理等部门通报的安全漏洞。对 CentOS 操作系统采取安全加固措施。及时修复网络安全等级测评、商用密码应用安全性评估、攻防演练、渗透测试、基线核查等发现的安全漏洞。

9.3 重要时期安全保障

按照河南省行政审批和政务信息管理局发布的《重要时期网络安全保障工作指南要求》及每年的重要时期网络安全保障工作提示的重保时间及范围开展重保工作，供应商需根据重保时间及范围制定重保方案，确保方案应科学全面可实施。保障前期各项准备工作完成，包括前期系统自查整改、系统侧安全设备策略优化、业务调整等内容；保障期间开展现场值班值守、业务运行监测、业务运行播报等内容；根据采购人提供的网络安全系统开展安全告警监测、分析研判、威胁定性与应急响应处置；重保结束后，全面回顾保障期间工作执行情况、安全攻击态势变化、处置成效及经验教训，形成重保总结报告。

9.4 安全合规检查

落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》《互联网政务应用安全管理规定》等法律法规管理制度规定组织开展安全合规检查。按照网络安全管理、保密管理、密码管理、公安、电子政务、行政审批和政务信息管理等部门通报完成安全检查。

9.5 上线前安全自查整改

功能新增或变更上线前，供应商须开展前置性安全自查。自查涵盖以下内容：利用自动化代码审计平台对上线及变更涉及的源代码进行静态分析，检查编码缺陷及安全漏洞；对系统引用的开源组件及第三方库进行成分分析，识别高危漏洞；利用漏洞扫描工具进行自动化检测，协助发现常见的 Web 漏洞和主机漏洞；变更涉及新服务器、新中间件或新数据库环境部署，需对该环境的核心配置项进行自动化核查，识别不符合通用安全基线的配置项。检查结束后出具安全评估报告，对识别出的高风险项提供可行性整改建议，并按照整改建议进行整改，整改后出具复测报告。

9.6 应急演练

定期开展应急演练，提升系统的应急响应能力与防护处置能力。服务期内至少组织开展2次实战模拟演练,重点验证应急响应流程的可行性及各岗位人员的响应联动效率。演练工作包含方案编制、场景模拟与过程记录。演练前需提交《应急演练工作方案》，

内容应包含演练目标、演练范围、演练场景设计、参与人员及职责分工、演练流程及时间安排、保障措施及风险控制措施；演练结束后提交《应急演练评估报告》，内容应包含演练过程回顾、演练目标达成情况、预案执行有效性评估、暴露的流程衔接问题与人员能力短板、针对性的预案优化建议及后续改进计划。

9.7 安全体检

服务期内供应商应按系统开展至少 1 次网络安全体检，涵盖资产摸排、脆弱性与合规差距识别。每次体检工作涵盖以下内容：对资产进行全量梳理；对操作系统、数据库及中间件的核心配置项进行自动化检查，识别不符合安全基线规范的配置项；通过模拟攻击手法对系统进行深度渗透测试，验证系统防御能力的薄弱环节；针对核心业务代码进行源代码缺陷扫描，协助发现编码规范问题。针对检查结果出具专业分析报告，对识别出的高风险项提供可行性整改建议，并视采购人需求配合进行整改后的复测验证。

9.8 其他方面

配合省级数字政府“一道墙”安全运营支撑平台开展安全漏洞扫描，每季度开展一次，共四次,并基于扫描情况完成漏洞整改和反馈工作。完成 AGENT 部署,对于未使用加密网关加密项目,需同步提供出入口 nginx 服务器名单,开通网络策略,一并将监测数据传输到省级数字政府“一道墙”安全运营支撑平台。完成系统资产调研表的反馈及动态更新,按照统一提供的资产调研表模板进行梳理、填写及调整核验工作,确保运维保障系统资产信息的完整性和准确性。组织专业技术人员在国家攻防演练和省级攻防演练期间进行值班值守，发现网络安全攻击及时报告并处置。落实《河南省行政审批和政务信息管理局网络安全事件应急预案》要求，发生安全事件后第一时间组织专业技术人员进行分析研判，及时报告并处置。

10.项目实施要求

运维要求	
一线运维	维护河南省省级一体化政务服务平台及运行环境稳定运行，负责平台巡检、变更等日常运维工作，并对系统的监控管理系统进行优化改造。
系统业务运维	保障河南省省级一体化政务服务平台上线事项正常使用，对接相关厅局业务系统，及时发现并解决用户注册登录、事项、办件、好差评、证照、数据共享等业务运行异常问题；确认

	因业务变更、流程改进或新增功能等而产生的需求，并根据实际需求对上线事项进行更新、升级。
基础环境运维	维护河南省省级一体化政务服务平台及运行环境稳定运行，及时发现并解决系统故障，保证系统稳定性及业务连续性。定期对系统进行全面检查，优化系统软件，记录系统运行情况，做好系统日志维护及运维文档管理。对系统运行过程中存在的问题进行完善修改，及时发布升级需求，完成系统版本升级。根据需要，开展重大配置变更、问题咨询和处理等工作。
数据库运维	监控数据库及依赖环境的运行，定期修复数据库漏洞，及时发现并解决数据库异常。根据软硬件资源使用及运行情况，定期评估数据库运行效率，优化参数配置。开展数据库安装、优化、初始化等工作。按照采购人要求，开展数据录入、处理、备份、更新以及数据提取、处理等工作。
系统安全运维	保障河南省省级一体化政务服务平台（一期）（除电子证照系统）网络和数据安全，开展日常安全监测、安全漏洞修复、重要时期安全保障、安全合规检查、上线前安全自查整改、应急演练、安全体检等工作。
数据分类分级	参照《数据安全技术 数据分类分级规则》(GB/T43697—2024)《全国一体化政务大数据体系 政务数据目录 第3部分：政务数据分类》（征求意见稿）和河南省一体化政务大数据体系工程标准《政务数据 分类分级指南》完成系统生成数据的分类分级梳理工作，系统汇聚的数据按照行业上级业务指导部门制定的数据分类分级要求开展数据分类分级工作。

11.驻场运维人数及要求

在合同约定服务期内，本项目要求提供不少于12人（其中业务系统运维不少于8人）的驻场运维服务，并应具备根据实际需要临时增配驻场运维人员的条件，运维人员对本系统运行维护工作提供全年的7x24小时的保障服务，工作日提供5x8小时的现场保障服务，保证系统稳定运行。驻场运维人员常驻采购人指定办公场地，并通过现场电话、微信等多种方式实现问题处理。

A 包：河南省政务服务移动端“豫事办”(一期)采购需求

河南省政务服务移动端“豫事办”（一期）包括移动端 APP，支付宝小程序、微信公众号以及采购人认定的支撑“豫事办”运行的其他软件或系统统称为“豫事办”平台。运维工作应对业务系统、信息资产和安全资产进行全面梳理，形成《系统及功能清单》、《系统资产清单》和《安全资产清单》，以资产清单为依托，开展基础环境运维、软件运维工作，以及各业务子系统的信息资源维护、短信发送服务，配合开展信息安全等级测评工作。具体运维需求如下：

1、基础环境及软件运维

根据实际运维工作需要，对平台的主机、数据库、中间件和业务系统的运行状态和性能指标进行监控，对运行日志进行采集和存储，并可提供日志查询和统计分析。主要运维要求：保障平台 7×24 小时不间断运行，针对基础环境运维保障系统总体可用率不低于 99.9%，日志保存时间不低于 180 天，运维期内无重大故障发生，无重大安全事故发生。

1.1 服务器运维内容

服务器日常运维。对新下发的服务器完成操作系统初始化、操作系统优化、操作系统安全加固、接入运维管理工具和日志采集平台等工作；对下发的漏洞扫描结果在规定时间内完成服务器漏洞修复，保障高危漏洞 3 日内完成修复，中危漏洞 7 日内完成修复，漏洞修复较复杂的应在 3 日内制定详尽的漏洞修复方案，报送采购人审批通过后，按照方案执行。

服务器运行监控。对服务器运行状态进行日常监测、对预警问题按照问题处理规范进行问题记录、流转、处理和跟踪等工作，建立健全的系统问题处理机制和规范，保障主机长期处于最优状态。在采购人界定的问题程度下，一般问题 2 个小时解决并记录，较严重问题 4 个小时出具问题解决方案并提交给采购人研判解决。

服务器资源全生命周期管理。对现有资源进行全面梳理，全面管理资源的申请、调整、释放工作。

1.2 中间件运维内容

中间件安装和漏洞修复。根据实际工作要求完成所需中间件的安装、集群搭建、优化、配置、调试和安全加固等工作，开展问题定位排查处理。在采购人界定的问题分类下，一般问题 2 小时内解决，较严重问题 4 小时内出具问题解决方案并提交给采购人研

判解决。

中间件运行监控。每日开展中间件的系统监控和问题处理工作，保障中间件长期处于最优状态。

1.3 数据库运维内容

数据库安装和漏洞修复。根据实际工作要求完成 Oracle、Mysql、Redis、ES、达梦等常用数据库部署、集群的搭建、配置和优化工作；数据库漏洞应在 2 日内编写详细的漏洞修复方案，提报给采购人研判，并按要求完成数据库安全加固和整改，保障数据库的稳定运行。

数据库运行监控。针对数据库运行状态进行全面监测，监控指标包括数据库运行指标、集群监控指标、表空间使用情况、慢 SQL 指标，对发现的问题应在 2 小时内进行定位并协调相关方处理，保障数据库长期处于最优状态。

数据库备份恢复和扩容。按照备份管理要求，对数据库进行备份和巡检。

1.4 日常巡检要求内容

做好系统资源日常监控，按政务云要求优化系统资源使用，需进行配置变更时，提供资源变更申请，做好系统资源变更后运行监控。提供每日不低于 1 次的操作系统、中间件、数据库、业务系统等运行指标、应用进程运行情况巡检工作，对预警和发现的问题和隐患，提出处理建议或修复方案，并及时处理，一般问题 2 个小时解决，较严重问题协调相关人员 4 个小时出具问题解决方案并提交给采购人研判解决。

1.5 运行情况报告内容

月度运维报告。根据业务系统业务办理情况，关键核心业务接口、数据接口调用量，用户量、注册用户数、访问人数，基础环境等运行情况及异常信息，出具业务系统运行报告；对运维工作进行梳理，出具运维月报；根据系统监控数据，对服务器的负载综合分析，出具服务器负载报告；根据数据库运行监控数据，组织数据库运维人员对数据库进行全面检查和综合评估，按月出具数据库健康状态报告，包括数据库部署运行情况、数据库备份情况，慢 SQL 数据情况、数据库优化建议。

季度运维报告。每季度进行系统运行和运维工作总结，提交季度系统运行工作报告，内容包括本季度内的系统运行情况，运维工作情况，需求完成情况，故障及处理情况，安全工作开展情况，其他需要汇报或讨论的内容及下个季度的工作计划等。

年度汇报。每年度进行系统运行和运维工作总结，提交年度系统运行工作报告，内容包括本年内的系统运行情况，运维工作情况，故障处理情况，安全工作开展情况，其

他需要汇报或讨论的内容及下个周期工作计划等。

1.6 网络软硬件维保服务

对安全设备的安全识别库、入侵特征库、病毒检测特征库等升级服务、定期设备巡检、故障处理修复、版本升级、设备保修服务。

2.业务系统运维

2.1 平台运维

每日对移动开发平台、移动应用管理平台、移动端发布管理、自动化部署、统一日志服务、国办事项接口服务、移动端事项接口服务及其他“豫事办”平台相关的运行指标、应用进程等运行情况进行巡检，对预警、故障和存在隐患及时处理,保障“豫事办”平台稳定运行。

2.2 服务应用维护

针对“豫事办”平台服务应用进行运维，保障服务应用稳定运行，运维内容包括但不限于服务应用运行状态巡检，故障排查处理，根据业务变化修改优化服务应用，按要求开展服务应用审核、测试、上下线等。

2.3 系统配置维护

按需对“豫事办”平台通知公告、轮播图、热门位、UI、VI 或其他配置进行运维，运维内容包括但不限于“豫事办”平台 UI 和 VI 维护，热门应用推荐配置，通知公告页面运营活动轮播图、热门位图标的设计等工作。

2.4 系统软件维护

按照采购人要求，完成“豫事办”平台软件的调整优化等工作，开展相关工作时需要制定技术方案，待采购人审核通过后按照规范流程具体实施并做好测试验证。

2.5 系统功能维护

根据业务需求对信息系统的功能进行优化调整，包括但不限于便民服务事项应用接入；分厅服务事项增加、调整；分厅布局、专区、组织机构增加、调整等，确保系统功能满足业务人员的工作需求。推动高频应用服务在“豫事办”苹果手机、鸿蒙手机、微信小程序端同步提供服务。

3.数据分类分级

参照《数据安全技术 数据分类分级规则》（GB/T43697—2024）《全国一体化政务大数据体系 政务数据目录 第 3 部分：政务数据分类》（征求意见稿）和河南省一体化政务大数据体系工程标准《政务数据 分类分级指南》完成系统生成数据的分类分级梳

理工作，系统汇聚的数据按照行业上级业务指导部门制定的数据分类分级要求开展数据分类分级工作。

4.安全运维

4.1 日常安全监测

组织专业技术力量，依托省级数字政府“一道墙”安全运营支撑平台、电子政务外网态势感知平台和自身监测能力，对河南省政务服务移动端“豫事办”(一期)系统进行7×24小时监测，分析研判系统面临的网络安全攻击，对可能发生的网络安全、数据安全隐患进行处置，确保系统安全稳定运行。

4.2 安全漏洞修复

及时修复网络安全管理、保密管理、密码管理、公安、电子政务、行政审批和政务信息管理等部门通报的安全漏洞。对CentOS操作系统采取安全加固措施。及时修复网络安全等级测评、商用密码应用安全性评估、攻防演练、渗透测试、基线核查等发现的安全漏洞。

4.3 重要时期安全保障

按照河南省行政审批和政务信息管理局发布的《重要时期网络安全保障工作指南要求》及每年的重要时期网络安全保障工作提示的重保时间及范围开展重保工作，供应商需根据重保时间及范围制定重保方案，确保方案应科学全面可实施。保障前期各项准备工作完成，包括前期系统自查整改、系统侧安全设备策略优化、业务调整等内容；保障期间开展现场值班值守、业务运行监测、业务运行播报等内容；根据采购人提供的网络安全系统开展安全告警监测、分析研判、威胁定性与应急响应处置；重保结束后，全面回顾保障期间工作执行情况、安全攻击态势变化、处置成效及经验教训，形成重保总结报告。

4.4 安全合规检查

落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》《互联网政务应用安全管理规定》等法律法规管理制度规定组织开展安全合规检查。按照网络安全管理、保密管理、密码管理、公安、电子政务、行政审批和政务信息管理等部门通报完成安全检查。

4.5 上线前安全自查整改

功能新增或变更上线前，供应商须开展前置性安全自查。自查涵盖以下内容：利用自动化代码审计平台对上线及变更涉及的源代码进行静态分析，检查编码缺陷及安全漏

洞；对系统引用的开源组件及第三方库进行成分分析，识别高危漏洞；利用漏洞扫描工具进行自动化检测，协助发现常见的 Web 漏洞和主机漏洞；变更涉及新服务器、新中间件或新数据库环境部署，需对该环境的核心配置项进行自动化核查，识别不符合通用安全基线的配置项。检查结束后出具安全评估报告，对识别出的高风险项提供可行性整改建议，并按照整改建议进行整改，整改后出具复测报告。

4.6 应急演练

定期开展应急演练，提升系统的应急响应能力与防护处置能力。服务期内至少组织开展2次实战模拟演练,重点验证应急响应流程的可行性及各岗位人员的响应联动效率。演练工作包含方案编制、场景模拟与过程记录。演练前需提交《应急演练工作方案》，内容应包含演练目标、演练范围、演练场景设计、参与人员及职责分工、演练流程及时间安排、保障措施及风险控制措施；演练结束后提交《应急演练评估报告》，内容应包含演练过程回顾、演练目标达成情况、预案执行有效性评估、暴露的流程衔接问题与人员能力短板、针对性的预案优化建议及后续改进计划。

4.7 安全体检

服务期内供应商应按系统开展至少 1 次网络安全体检，涵盖资产摸排、脆弱性与合规差距识别。每次体检工作涵盖以下内容：对资产进行全量梳理；对操作系统、数据库及中间件的核心配置项进行自动化检查，识别不符合安全基线规范的配置项；通过模拟攻击手法对系统进行深度渗透测试，验证系统防御能力的薄弱环节；针对核心业务代码进行源代码缺陷扫描，协助发现编码规范问题。针对检查结果出具专业分析报告，对识别出的高风险项提供可行性整改建议，并视采购人需求配合进行整改后的复测验证。

4.8 其他方面

配合省级数字政府“一道墙”安全运营支撑平台开展安全漏洞扫描，每季度开展一次，共四次,并基于扫描情况完成漏洞整改和反馈工作。完成 AGENT 部署,对于未使用加密网关加密项目,需同步提供出入口 nginx 服务器名单,开通网络策略,一并将监测数据传输到省级数字政府“一道墙”安全运营支撑平台。完成系统资产调研表的反馈及动态更新,按照统一提供的资产调研表模板进行梳理、填写及调整核验工作,确保运维保障系统资产信息的完整性和准确性。组织专业技术人员在国家攻防演练和省级攻防演练期间进行值班值守，发现网络安全攻击及时报告并处置。落实《河南省行政审批和政务信息管理局网络安全事件应急预案》要求，发生安全事件后第一时间组织专业技术人员进行分析研判，及时报告并处置。

5.项目实施要求

运维要求	
一线运维	维护业务系统及基础环境稳定运行，负责系统巡检、变更等日常运维工作，并对监控管理系统进行调整优化。记录系统运行及故障处置情况，做好系统日常维护及运维文档管理。
业务系统运维	保障业务系统稳定运行。对接相关业务系统，及时发现并解决服务应用运行异常问题，服务应用正常使用:确认因业务变更、流程改进或新增功能等而产生的需求，并根据实际需求进行更新、升级;配合进行服务应用审核、测试、上下线等;对通知公告、轮播图、热门位、UI、VI等配置进行维护;根据需求对业务系统进行调整优化；及时发现业务系统存在的问题进行完善修改，发布升级需求并完成升级。
基础环境运维	维护系统及基础运行环境稳定运行，及时发现并解决系统故障保证系统稳定性及业务连续性。对服务器等资产进行全周期管理:定期对系统进行全面检查，优化系统软件，记录系统运行情况做好系统日常维护及运维文档管理:修复各类安全漏洞:配合完成安全设备或软件的配置调试、调整优化等工作:根据需要，开展重大配置变更、问题咨询和处理等工作。
数据库运维	监控数据库及依赖环境的运行，定期修复数据库漏洞，及时发现并解决数据库故障问题。根据软硬件资源使用及运行情况，定期评估数据库运行效率，优化参数配置。开展数据库安装、优化、初始化，备份、备份恢复验证、问题处理等工作。按照数据库运行情况，出具数据库运行状况报告，
系统安全运维	保障河南省政务服务移动端“豫事办”(一期)网络和数据安全，开展日常安全监测、安全漏洞修复、重要时期安全保障、安全合规检查、上线前安全自查整改、应急演练、安全体检等工作。

数据分类分级	参照《数据安全技术 数据分类分级规则》（GB/T43697—2024）《全国一体化政务大数据体系 政务数据目录 第3部分：政务数据分类》（征求意见稿）和河南省一体化政务大数据体系工程标准《政务数据 分类分级指南》完成系统生成数据的分类分级梳理工作，系统汇聚的数据按照行业上级业务指导部门制定的数据分类分级要求开展数据分类分级工作。

6.驻场运维人数及要求

在合同约定服务期内，本项目要求提供不少于 4 人的驻场运维服务，运维人员对本系统运行维护工作提供全年的 7x24 小时的保障服务，工作日提供 5x8 小时的现场保障服务，保证系统稳定运行。驻场运维人员常驻采购人指定办公场地，并通过现场电话、微信等多种方式实现问题处理。

A 包：河南省“豫正通”（一期）采购需求

河南省“豫正通”(一期)运维工作应对业务系统、信息资产和安全资产进行全面梳理，形成《系统及功能清单》《系统资产清单》和《安全资产清单》，以资产清单为依托，开展基础环境运维、软件运维工作，以及各业务子系统的信息资源维护，配合开展信息安全等级测评和商用密码应用安全性评估工作。具体运维需求如下：

1.基础环境及软件运维

根据实际运维工作需要，对平台的主机、数据库、中间件和业务系统的运行状态和性能指标进行监控，对运行日志进行采集和存储，并可提供日志查询和统计分析。主要运维要求：保障平台 7×24 小时不间断运行，针对基础环境运维保障系统总体可用率不低于 99.9%，日志保存时间不低于 180 天，运维期内无重大故障发生，无重大安全事故发生。

1.1 服务器运维内容

服务器日常运维。对新下发的服务器完成操作系统初始化、操作系统优化、操作系统安全加固、接入运维管理工具和日志采集平台等工作；对下发的漏洞扫描结果在规定时间内完成服务器漏洞修复，保障高危漏洞 3 日内完成修复，中危漏洞 7 日内完成修复，漏洞修复较复杂的应在 3 日内制定详尽的漏洞修复方案，报送采购人审批通过后，按照方案执行。

服务器运行监控。对服务器运行状态进行日常监测、对预警问题按照问题处理规范进行问题记录、流转、处理和跟踪等工作，建立健全的系统问题处理机制和规范，保障主机长期处于最优状态。在采购人界定的问题程度下，一般问题 2 个小时解决并记录，较严重问题 4 个小时出具问题解决方案并提交给采购人研判解决。

服务器资源全生命周期管理。对现有资源进行全面梳理，全面管理资源的申请、调整、释放工作。

1.2 中间件运维内容

中间件安装和漏洞修复。根据实际工作要求完成所需中间件的安装、集群搭建、优化、配置、调试和安全加固等工作，开展问题定位排查处理。在采购人界定的问题分类下，一般问题 2 小时内解决，较严重问题 4 小时内出具问题解决方案并提交给采购人研判解决。

中间件运行监控。每日开展中间件的系统监控和问题处理工作，保障中间件长期处

于最优状态。

1.3 数据库运维内容

数据库安装和漏洞修复。根据实际工作要求完成 Oracle、Mysql、Redis、ES、达梦等常用数据库部署、集群的搭建、配置和优化工作；数据库漏洞应在 2 日内编写详细的漏洞修复方案，提报给采购人研判，并按要求完成数据库安全加固和整改，保障数据库的稳定运行。

数据库运行监控。针对数据库运行状态进行全面监测，监控指标包括数据库运行指标、集群监控指标、表空间使用情况、慢 SQL 指标，对发现的问题应在 2 小时内进行定位并协调相关方处理，保障数据库长期处于最优状态。

数据库备份恢复和扩容。按照备份管理要求，对数据库进行备份和巡检。

1.4 日常巡检要求内容

做好系统资源日常监控，按政务云要求优化系统资源使用，需进行配置变更时，提供资源变更申请，做好系统资源变更后运行监控。提供每日不低于 1 次的操作系统、中间件、数据库、业务系统等运行指标、应用进程运行情况巡检工作，对预警和发现的问题和隐患，提出处理建议或修复方案，并及时处理，一般问题 2 个小时解决，较严重问题协调相关人员 4 个小时出具问题解决方案并提交给采购人研判解决。

1.5 运行情况报告内容

月度运维报告。根据业务系统运行情况和业务办理量、用户量、注册用户数、访问人数等信息，出具业务系统运行报告；对运维工作进行梳理，出具运维月报；根据系统监控数据，对服务器的负载综合分析，出具服务器负载报告；根据数据库运行监控数据，组织数据库运维人员对数据库进行全面检查和综合评估，按月出具数据库健康状态报告，包括数据库部署运行情况、数据库备份情况，慢 SQL 数据情况、数据库优化建议。

季度运维报告。每季度进行系统运行和运维工作总结，提交季度系统运行工作报告，内容包括本季度内的系统运行情况，运维工作情况，需求完成情况，故障及处理情况，安全工作开展情况，其他需要汇报或讨论的内容及下个季度的工作计划等。

年度汇报。每年度进行系统运行和运维工作总结，提交年度系统运行工作报告，内容包括本年内的系统运行情况，运维工作情况，故障处理情况，安全工作开展情况，其他需要汇报或讨论的内容及下个周期工作计划等。

1.6 网络软硬件维保服务

对安全设备的安全识别库、入侵特征库、病毒检测特征库等升级服务、定期设备巡

检、故障处理修复、版本升级、设备保修服务。

2.业务系统运维

河南省“豫正通”平台主要包含“豫快办”、应急指挥、经济运行、领导关注、领导批示、厅局直通、市县直达、一键直联和个人中心等9个重点应用模块APP端及用户统一管理平台、豫快办督办平台、信息报送系统、指标填报系统等4个管理系统。

业务系统运维主要包含对接省委、省政府及相关厅局，及时发现并解决用户注册登录、信息报送、信息发布、指标填报等业务问题；定期对业务系统运行情况进行巡检，记录系统运行情况，做好系统运维文档管理。同时，按照省委要求，协助省委办公厅处理日常值班报告、豫快办和领导重点交办事项等信息资源维护工作。

3.数据分类分级

参照《数据安全技术 数据分类分级规则》（GB/T43697—2024）《全国一体化政务大数据体系 政务数据目录 第3部分：政务数据分类》（征求意见稿）和河南省一体化政务大数据体系工程标准《政务数据 分类分级指南》完成系统生成数据的分类分级梳理工作，系统汇聚的数据按照行业上级业务指导部门制定的数据分类分级要求开展数据分类分级工作。

4.安全运维

4.1 日常安全监测

组织专业技术力量，依托省级数字政府“一道墙”安全运营支撑平台、电子政务外网态势感知平台和自身监测能力，对河南省“豫正通”（一期）系统进行7×24小时监测，分析研判系统面临的网络安全攻击，对可能发生的网络安全、数据安全隐患进行处置，确保系统安全稳定运行。

4.2 安全漏洞修复

及时修复网络安全管理、保密管理、密码管理、公安、电子政务、行政审批和政务信息管理等部门通报的安全漏洞。及时修复网络安全等级测评、商用密码应用安全性评估、攻防演练、渗透测试、基线核查等发现的安全漏洞。

4.3 重要时期安全保障

按照河南省行政审批和政务信息管理局发布的《重要时期网络安全保障工作指南要求》及每年的重要时期网络安全保障工作提示的重保时间及范围开展重保工作，供应商需根据重保时间及范围制定重保方案，确保方案应科学全面可实施。保障前期各项准备

工作完成，包括前期系统自查整改、系统侧安全设备策略优化、业务调整等内容；保障期间开展现场值班值守、业务运行监测、业务运行播报等内容；根据采购人提供的网络安全系统开展安全告警监测、分析研判、威胁定性与应急响应处置；重保结束后，全面回顾保障期间工作执行情况、安全攻击态势变化、处置成效及经验教训，形成重保总结报告。

4.4 安全合规检查

落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》《互联网政务应用安全管理规定》等法律法规管理制度规定组织开展安全合规检查。按照网络安全管理、保密管理、密码管理、公安、电子政务、行政审批和政务信息管理等部门通报完成安全检查。

4.5 上线前安全自查整改

功能新增或变更上线前，供应商须开展前置性安全自查。自查涵盖以下内容：利用自动化代码审计平台对上线及变更涉及的源代码进行静态分析，检查编码缺陷及安全漏洞；对系统引用的开源组件及第三方库进行成分分析，识别高危漏洞；利用漏洞扫描工具进行自动化检测，协助发现常见的 Web 漏洞和主机漏洞；变更涉及新服务器、新中间件或新数据库环境部署，需对该环境的核心配置项进行自动化核查，识别不符合通用安全基线的配置项。检查结束后出具安全评估报告，对识别出的高风险项提供可行性整改建议，并按照整改建议进行整改，整改后出具复测报告。

4.6 应急演练

定期开展应急演练，提升系统的应急响应能力与防护处置能力。服务期内至少组织开展2次实战模拟演练,重点验证应急响应流程的可行性及各岗位人员的响应联动效率。演练工作包含方案编制、场景模拟与过程记录。演练前需提交《应急演练工作方案》，内容应包含演练目标、演练范围、演练场景设计、参与人员及职责分工、演练流程及时间安排、保障措施及风险控制措施；演练结束后提交《应急演练评估报告》，内容应包含演练过程回顾、演练目标达成情况、预案执行有效性评估、暴露的流程衔接问题与人员能力短板、针对性的预案优化建议及后续改进计划。

4.7 安全体检

服务期内供应商应按系统开展至少 1 次网络安全体检，涵盖资产摸排、脆弱性与合规差距识别。每次体检工作涵盖以下内容：对资产进行全量梳理；对操作系统、数据库及中间件的核心配置项进行自动化检查，识别不符合安全基线规范的配置项；通过模拟

攻击手法对系统进行深度渗透测试，验证系统防御能力的薄弱环节；针对核心业务代码进行源代码缺陷扫描，协助发现编码规范问题。针对检查结果出具专业分析报告，对识别出的高风险项提供可行性整改建议，并视采购人需求配合进行整改后的复测验证。

4.8 其他方面

配合省级数字政府“一道墙”安全运营支撑平台开展安全漏洞扫描，每季度开展一次，共四次,并基于扫描情况完成漏洞整改和反馈工作。完成 AGENT 部署,对于未使用加密网关加密项目,需同步提供出入口 nginx 服务器名单,开通网络策略,一并将监测数据传输到省级数字政府“一道墙”安全运营支撑平台。完成系统资产调研表的反馈及动态更新,按照统一提供的资产调研表模板进行梳理、填写及调整核验工作,确保运维保障系统资产信息的完整性和准确性。组织专业技术人员在国家攻防演练和省级攻防演练期间进行值班值守，发现网络安全攻击及时报告并处置。落实《河南省行政审批和政务信息管理局网络安全事件应急预案》要求，发生安全事件后第一时间组织专业技术人员进行分析研判，及时报告并处置。

5.项目实施要求

运维要求	
基础环境运维	维护河南省“豫正通”（一期）项目及运行环境稳定运行，及时发现并解决系统故障，保证系统稳定性及业务连续性。定期对系统进行全面检查，优化系统软件，记录系统基础环境运行情况，做好系统日志维护及运维文档管理。
系统业务运维	保障河南省“豫正通”（一期）平台正常使用，对接省委、省政府及相关厅局，及时发现并解决用户注册登录、信息报送、信息发布、指标填报等业务问题；定期对业务系统运行情况进行巡检，记录系统运行情况，做好系统运维文档管理。
系统安全运维	保障河南省“豫正通”（一期）网络和数据安全，开展日常安全监测、安全漏洞修复、重要时期安全保障、安全合规检查、上线前安全自查整改、应急演练、安全体检等工作。

数据分类分级	参照《数据安全技术 数据分类分级规则》（GB/T43697—2024）《全国一体化政务大数据体系 政务数据目录 第3部分：政务数据分类》（征求意见稿）和河南省一体化政务大数据体系工程标准《政务数据 分类分级指南》完成系统生成数据的分类分级梳理工作，系统汇聚的数据按照行业上级业务指导部门制定的数据分类分级要求开展数据分类分级工作。

6.驻场运维人数及要求

在合同约定服务期内，本项目要求提供不少于 3 人的驻场运维服务（包含省委驻场 2 人），运维人员对本系统运行维护工作提供全年的 7x24 小时的保障服务，工作日提供 5x8 小时的现场保障服务，保证系统稳定运行。驻场运维人员常驻采购人指定办公场地，并通过现场电话、微信等多种方式实现问题处理。

A 包：河南省“互联网+监管”系统（一期）采购需求

河南省“互联网+监管”系统（一期）运维工作应对业务系统、信息资产和安全资产进行全面梳理，形成《系统及功能清单》、《系统资产清单》和《安全资产清单》，以资产清单为依托，开展基础环境运维、软件运维工作，以及各业务子系统的信息资源维护，配合开展信息安全等级测评工作。具体运维需求如下：

1.基础环境及软件运维

根据实际运维工作需要，对平台的主机、数据库、中间件和业务系统的运行状态和性能指标进行监控，对运行日志进行采集和存储，并可提供日志查询和统计分析。主要运维要求：保障平台 7×24 小时不间断运行，针对基础环境运维保障系统总体可用率不低于 99.9%，日志保存时间不低于 180 天，运维期内无重大故障发生，无重大安全事故发生。

1.1 服务器运维内容

服务器日常运维。对新下发的服务器完成操作系统初始化、操作系统优化、操作系统安全加固、接入运维管理工具和日志采集平台等工作；对下发的漏洞扫描结果在规定时间内完成服务器漏洞修复，保障高危漏洞 3 日内完成修复，中危漏洞 7 日内完成修复，漏洞修复较复杂的应在 3 日内制定详尽的漏洞修复方案，报送采购人审批通过后，按照方案执行。

服务器运行监控。对服务器运行状态进行日常监测、对预警问题按照问题处理规范进行问题记录、流转、处理和跟踪等工作，建立健全的系统问题处理机制和规范，保障主机长期处于最优状态。在采购人界定的问题程度下，一般问题 2 个小时解决并记录，较严重问题 4 个小时出具问题解决方案并提交给采购人研判解决。

服务器资源全生命周期管理。对现有资源进行全面梳理，全面管理资源的申请、调整、释放工作。

1.2 中间件运维内容

中间件安装和漏洞修复。根据实际工作要求完成所需中间件的安装、集群搭建、优化、配置、调试和安全加固等工作，开展问题定位排查处理。在采购人界定的问题分类下，一般问题 2 小时内解决，较严重问题 4 小时内出具问题解决方案并提交给采购人研判解决。

中间件运行监控。每日开展中间件的系统监控和问题处理工作，保障中间件长期处

于最优状态。

1.3 数据库运维内容

数据库安装和漏洞修复。根据实际工作要求完成 Oracle、Mysql、Redis、ES、达梦等常用数据库部署、集群的搭建、配置和优化工作；数据库漏洞应在 2 日内编写详细的漏洞修复方案，提报给采购人研判，并按要求完成数据库安全加固和整改，保障数据库的稳定运行。

数据库运行监控。针对数据库运行状态进行全面监测，监控指标包括数据库运行指标、集群监控指标、表空间使用情况、慢 SQL 指标，对发现的问题应在 2 小时内进行定位并协调相关方处理，保障数据库长期处于最优状态。

数据库备份恢复和扩容。按照备份管理要求，对数据库进行备份和巡检。根据数据库空间使用情况，及时协调相关方开展数据库扩容工作。

根据采购人数据调整工作要求对河南省“互联网+监管”系统（一期）数据库进行迁移。

1.4 日常巡检要求内容

做好系统资源日常监控，按政务云要求优化系统资源使用，需进行配置变更时，提供资源变更申请，做好系统资源变更后运行监控。提供每日不低于 1 次的操作系统、中间件、数据库、业务系统等运行指标、应用进程运行情况巡检工作，对预警和发现的问题和隐患，提出处理建议或修复方案，并及时处理，一般问题 2 个小时解决，较严重问题协调相关人员 4 个小时出具问题解决方案并提交给采购人研判解决。

1.5 运行情况报告内容

月度运维报告。根据业务系统运行情况和业务办理量、用户量、注册用户数、访问人数等信息，出具业务系统运行报告；对运维工作进行梳理，出具运维月报；根据系统监控数据，对服务器的负载综合分析，出具服务器负载报告；根据数据库运行监控数据，组织数据库运维人员对数据库进行全面检查和综合评估，按月出具数据库健康状态报告，包括数据库部署运行情况、数据库备份情况，慢 SQL 数据情况、数据库优化建议。

季度运维报告。每季度进行系统运行和运维工作总结，提交季度系统运行工作报告，内容包括本季度内的系统运行情况，运维工作情况，需求完成情况，故障及处理情况，安全工作开展情况，其他需要汇报或讨论的内容及下个季度的工作计划等。

年度汇报。每年度进行系统运行和运维工作总结，提交年度系统运行工作报告，内容包括本年内的系统运行情况，运维工作情况，故障处理情况，安全工作开展情况，其

他需要汇报或讨论的内容及下个周期工作计划等。

1.6 网络软硬件维保服务

对安全设备的安全识别库、入侵特征库、病毒检测特征库等升级服务、定期设备巡检、故障处理修复、版本升级、设备保修服务。

2.业务系统运维

每日对监管数据中心、监管门户界面系统、监管事项清单动态管理系统、行政执法监管应用系统、风险预警系统、分析评价系统、监管可视化系统、监管数据填报系统、监管数据治理系统的运行指等运行情况进行巡检，对预警、故障和存在隐患及时处理，保障“互联网+监管”系统（一期）稳定运行。

按照采购人要求，完成“互联网+监管”系统（一期）软件的调整优化等工作，开展相关工作时需要制定技术方案，待采购人审核通过后按照规范流程具体实施并做好测试验证。

3.信息资源维护

3.1 数据需求沟通

基于国办下发的监管数据标准规范，结合厅局、地市及采购人的数据需求，形成数据需求材料并进行确认。

3.2 监管数据汇聚

数据汇聚方案。结合当地市、厅局的具体数据内容情况，讨论制定汇聚方案，依托省数据共享交换平台将数据按照监管数据标准规范抽取至项目使用的省数据共享交换平台分配前置机上对应的数据库表，保证数据及时汇聚和完整性。

数据抽取任务和转换。采用库表形式进行交换，配置数据增量抽取任务。

3.3 数据上报

监管数据经过质量治理后，通过省数据共享交换平台将不符合国家标准规范的数据下发地市、厅局前置机或填报系统，并下发数据详细错误信息，要求对错误数据进行整改并再次上传。对质检后符合标准规范的数据配置数据上报任务，上报至前置机，确认数据是否准确上报。

3.4 数据指标

参照国办对地方的监管数据考核指标，结合系统数据汇聚内容，梳理地方数据对接考核统计表，包括监管行为覆盖率、风险线索、数据准确率、数据更新占比。

3.5 数据问题解答

地市、厅局对监管数据考核指标的统计口径及数据汇聚情况问题；解答地市、厅局对监管行为数据覆盖率疑问；整理关于数据汇聚及数据统计常见问题，在工作门户发布并动态更新。

3.6 系统对接

根据河南省18个地市实际情况和对接需求，按照河南省“互联网+监管”系统（一期）系统对接标准提供用户中心对接技术服务，提供对接技术服务的宣贯和问题解答。

3.7 数据分类分级

参照《数据安全技术 数据分类分级规则》（GB/T43697—2024）《全国一体化政务大数据体系 政务数据目录 第3部分：政务数据分类》（征求意见稿）和河南省一体化政务大数据体系工程标准《政务数据 分类分级指南》完成系统生成数据的分类分级梳理工作，系统汇聚的数据按照行业上级业务指导部门制定的数据分类分级要求开展数据分类分级工作。

4.安全运维

4.1 日常安全监测

组织专业技术力量，依托省级数字政府“一道墙”安全运营支撑平台、电子政务外网态势感知平台和自身监测能力，对河南省“互联网+监管”系统（一期）系统进行7×24小时监测，分析研判系统面临的网络安全攻击，对可能发生的网络安全、数据安全隐患进行处置，确保系统安全稳定运行。

4.2 安全漏洞修复

及时修复网络安全管理、保密管理、密码管理、公安、电子政务、行政审批和政务信息管理等部门通报的安全漏洞。对CentOS操作系统采取安全加固措施。及时修复网络安全等级测评、商用密码应用安全性评估、攻防演练、渗透测试、基线核查等发现的安全漏洞。

4.3 重要时期安全保障

按照河南省行政审批和政务信息管理局发布的《重要时期网络安全保障工作指南要求》及每年的重要时期网络安全保障工作提示的重保时间及范围开展重保工作，供应商需根据重保时间及范围制定重保方案，确保方案应科学全面可实施。保障前期各项准备工作完成，包括前期系统自查整改、系统侧安全设备策略优化、业务调整等内容；保障

期间开展现场值班值守、业务运行监测、业务运行播报等内容；根据采购人提供的网络安全系统开展安全告警监测、分析研判、威胁定性与应急响应处置；重保结束后，全面回顾保障期间工作执行情况、安全攻击态势变化、处置成效及经验教训，形成重保总结报告。

4.4 安全合规检查

落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》《互联网政务应用安全管理规定》等法律法规管理制度规定组织开展安全合规检查。按照网络安全管理、保密管理、密码管理、公安、电子政务、行政审批和政务信息管理等部门通报完成安全检查。

4.5 上线前安全自查整改

功能新增或变更上线前，供应商须开展前置性安全自查。自查涵盖以下内容：利用自动化代码审计平台对上线及变更涉及的源代码进行静态分析，检查编码缺陷及安全漏洞；对系统引用的开源组件及第三方库进行成分分析，识别高危漏洞；利用漏洞扫描工具进行自动化检测，协助发现常见的 Web 漏洞和主机漏洞；变更涉及新服务器、新中间件或新数据库环境部署，需对该环境的核心配置项进行自动化核查，识别不符合通用安全基线的配置项。检查结束后出具安全评估报告，对识别出的高风险项提供可行性整改建议，并按照整改建议进行整改，整改后出具复测报告。

4.6 应急演练

定期开展应急演练，提升系统的应急响应能力与防护处置能力。服务期内至少组织开展2次实战模拟演练,重点验证应急响应流程的可行性及各岗位人员的响应联动效率。演练工作包含方案编制、场景模拟与过程记录。演练前需提交《应急演练工作方案》，内容应包含演练目标、演练范围、演练场景设计、参与人员及职责分工、演练流程及时间安排、保障措施及风险控制措施；演练结束后提交《应急演练评估报告》，内容应包含演练过程回顾、演练目标达成情况、预案执行有效性评估、暴露的流程衔接问题与人员能力短板、针对性的预案优化建议及后续改进计划。

4.7 安全体检

服务期内供应商应按系统开展至少 1 次网络安全体检，涵盖资产摸排、脆弱性与合规差距识别。每次体检工作涵盖以下内容：对资产进行全量梳理；对操作系统、数据库及中间件的核心配置项进行自动化检查，识别不符合安全基线规范的配置项；通过模拟攻击手法对系统进行深度渗透测试，验证系统防御能力的薄弱环节；针对核心业务代码

进行源代码缺陷扫描，协助发现编码规范问题。针对检查结果出具专业分析报告，对识别出的高风险项提供可行性整改建议，并视采购人需求配合进行整改后的复测验证。

4.8 其他方面

配合省级数字政府“一道墙”安全运营支撑平台开展安全漏洞扫描，每季度开展一次，共四次,并基于扫描情况完成漏洞整改和反馈工作。完成 AGENT 部署,对于未使用加密网关加密项目,需同步提供出入口 nginx 服务器名单,开通网络策略,一并将监测数据传输到省级数字政府“一道墙”安全运营支撑平台。完成系统资产调研表的反馈及动态更新,按照统一提供的资产调研表模板进行梳理、填写及调整核验工作,确保运维保障系统资产信息的完整性和准确性。组织专业技术人员在国家攻防演练和省级攻防演练期间进行值班值守，发现网络安全攻击及时报告并处置。落实《河南省行政审批和政务信息管理局网络安全事件应急预案》要求，发生安全事件后第一时间组织专业技术人员进行分析研判，及时报告并处置。

5.项目实施要求

运维要求	
系统业务运维	保障河南省“互联网+监管”系统（一期）正常使用，开展系统巡检、系统配置、问题答疑工作。及时发现并解决用户注册登录、信息填报等问题。
基础环境运维	维护河南省“互联网+监管”系统（一期）及运行环境稳定运行，及时发现并解决系统故障，保证系统稳定性及业务连续性。定期对系统进行全面检查，记录系统运行情况，做好系统日志维护及运维文档管理。
信息资源维护	根据国办下发的监管数据标准规范、河南省“互联网+监管”系统（一期）相关数据标准和对接规范进行数据需求沟通、数据汇聚、数据上报、数据指标、数据问题答疑、用户中心系统对接。
系统安全运维	保障河南省“互联网+监管”系统（一期）网络和数据安全，开展日常安全监测、安全漏洞修复、重要时期安全保障、安全合规检查、上线前安全自查整改、应急演练、安全体检等工作。

数据分类分级	参照《数据安全技术 数据分类分级规则》（GB/T43697—2024）《全国一体化政务大数据体系 政务数据目录 第3部分:政务数据分类》（征求意见稿）和河南省一体化政务大数据体系工程标准《政务数据 分类分级指南》完成系统生成数据的分类分级梳理工作，系统汇聚的数据按照行业上级业务指导部门制定的数据分类分级要求开展数据分类分级工作。

6.驻场运维人数及要求

在合同约定服务期内，本项目要求提供不少于2人的驻场运维服务，运维人员对本系统运行维护工作提供全年的7x24小时的保障服务，工作日提供5x8小时的现场保障服务，保证系统稳定运行。驻场运维人员常驻采购人指定办公场地，并通过现场电话、微信等多种方式实现问题处理。

A 包：内容安全监测项目采购需求

内容安全监测项目运维工作应对业务系统、信息资产和安全资产进行全面梳理，形成《系统及功能清单》《系统资产清单》和《安全资产清单》，以资产清单为依托，开展基础环境运维、软件运维工作，以及各业务子系统的信息资源维护。具体运维需求如下：

一、内容安全监测平台

内容安全监测平台部署在河南省信创云专有云上，主要通过接口对接方式，对政务云上非涉密政务信息系统进行在线内容安全监测。本项目采用驻场运维加远程支撑服务的运维模式。结合业务特点，建立流程化、规范化、专业化的运维支撑服务体系，提供技术咨询、告警研判、问题处置、平台优化等技术服务。保证平台业务 7×24 小时不间断运行。

平台运维主要包括业务系统日常运维、告警研判处置、线上线下结合的特定类型告警处置、服务器组件日常运维、数据备份和恢复、漏洞修复、故障处理、常规安全检查服务、系统功能优化、系统迁移等工作。

1.系统日常运维

涵盖从底层基础设施到上层应用的全栈式管理，具体范围包括但不限于：

1.1 基础设施运维

服务器、虚拟机、网络设备、存储设备的监控如出现问题，则组织排查具体的问题情况，协调我方和相关云资源提供单位处置问题，直至问题解决系统能够流畅运行为止。

1.2 平台软件运维

操作系统、数据库、中间件、备份软件的安装、配置、优化与补丁管理。

1.3 数据专项运维

数据库的日常管理、性能优化及数据业务支撑。

2.安全运维

2.1 日常安全监测

组织专业技术力量，依托省级数字政府“一道墙”安全运营支撑平台、电子政务外网态势感知平台和自身监测能力，对内容安全监测项目进行 7×24 小时监测，分析研判系统面临的网络安全攻击，对可能发生的网络安全、数据安全隐患进行处置，确保系统安全稳定运行。

2.2 安全漏洞修复

及时修复网络安全管理、保密管理、密码管理、公安、电子政务、行政审批和政务信息管理等部门通报的安全漏洞。及时修复网络安全等级测评、商用密码应用安全性评估、攻防演练、渗透测试、基线核查等发现的安全漏洞。

2.3 重要时期安全保障

按照河南省行政审批和政务信息管理局发布的《重要时期网络安全保障工作指南要求》及每年的重要时期网络安全保障工作提示的重保时间及范围开展重保工作，供应商需根据重保时间及范围制定重保方案，确保方案应科学全面可实施。保障前期各项准备工作完成，包括前期系统自查整改、系统侧安全设备策略优化、业务调整等内容；保障期间开展现场值班值守、业务运行监测、业务运行播报等内容；根据采购人提供的网络安全系统开展安全告警监测、分析研判、威胁定性与应急响应处置；重保结束后，全面回顾保障期间工作执行情况、安全攻击态势变化、处置成效及经验教训，形成重保总结报告。

2.4 安全合规检查

落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》《互联网政务应用安全管理规定》等法律法规管理制度规定组织开展安全合规检查。按照网络安全管理、保密管理、密码管理、公安、电子政务、行政审批和政务信息管理等部门通报完成安全检查。

2.5 上线前安全自查整改

功能新增或变更上线前，供应商须开展前置性安全自查。自查涵盖以下内容：利用自动化代码审计平台对上线及变更涉及的源代码进行静态分析，检查编码缺陷及安全漏洞；对系统引用的开源组件及第三方库进行成分分析，识别高危漏洞；利用漏洞扫描工具进行自动化检测，协助发现常见的Web漏洞和主机漏洞；变更涉及新服务器、新中间件或新数据库环境部署，需对该环境的核心配置项进行自动化核查，识别不符合通用安全基线的配置项。检查结束后出具安全评估报告，对识别出的高风险项提供可行性整改建议，并按照整改建议进行整改，整改后出具复测报告。

2.6 应急演练

定期开展应急演练，提升系统的应急响应能力与防护处置能力。服务期内至少组织开展2次实战模拟演练,重点验证应急响应流程的可行性及各岗位人员的响应联动效率。演练工作包含方案编制、场景模拟与过程记录。演练前需提交《应急演练工作方案》，

内容应包含演练目标、演练范围、演练场景设计、参与人员及职责分工、演练流程及时间安排、保障措施及风险控制措施；演练结束后提交《应急演练评估报告》，内容应包含演练过程回顾、演练目标达成情况、预案执行有效性评估、暴露的流程衔接问题与人员能力短板、针对性的预案优化建议及后续改进计划。

2.7 安全体检

服务期内供应商应按系统开展至少 1 次网络安全体检，涵盖资产摸排、脆弱性与合规差距识别。每次体检工作涵盖以下内容：对资产进行全量梳理；对操作系统、数据库及中间件的核心配置项进行自动化检查，识别不符合安全基线规范的配置项；通过模拟攻击手法对系统进行深度渗透测试，验证系统防御能力的薄弱环节；针对核心业务代码进行源代码缺陷扫描，协助发现编码规范问题。针对检查结果出具专业分析报告，对识别出的高风险项提供可行性整改建议，并视采购人需求配合进行整改后的复测验证。

2.8 其他方面

配合省级数字政府“一道墙”安全运营支撑平台开展安全漏洞扫描，每季度开展一次，共四次,并基于扫描情况完成漏洞整改和反馈工作。完成 AGENT 部署,对于未使用加密网关加密项目,需同步提供出入口 nginx 服务器名单,开通网络策略,一并将监测数据传输到省级数字政府“一道墙”安全运营支撑平台。完成系统资产调研表的反馈及动态更新,按照统一提供的资产调研表模板进行梳理、填写及调整核验工作,确保运维保障系统资产信息的完整性和准确性。组织专业技术人员在国家攻防演练和省级攻防演练期间进行值班值守，发现网络安全攻击及时报告并处置。落实《河南省行政审批和政务信息管理局网络安全事件应急预案》要求，发生安全事件后第一时间组织专业技术人员进行分析研判，及时报告并处置。

3. 业务系统运维

业务应用的部署、发布、监控及基础功能支持，定期监测和维护核心业务模块，如“标准化数据接口服务”等，确保系统能够稳定采集被监测业务平台流转文件和相关数据，保证系统运行流畅稳定。

4. 平台配置管理

保证平台能够满足不断变化的业务监测需求，需要对平台中的参数、策略、帐号等信息进行维护。根据用户要求完成对角色账号、部门信息、策略调整等内容的运维工作。根据业务的当前要求，完成相应参数的配置，保证监测工作流畅运行。

5.数据分类分级

参照《数据安全技术 数据分类分级规则》（GB/T43697—2024）《全国一体化政务大数据体系政务数据目录第3部分：政务数据分类》（征求意见稿）和河南省一体化政务大数据体系工程标准《政务数据分类分级指南》完成系统生成数据的分类分级梳理工作，系统汇聚的数据按照行业上级业务指导部门制定的数据分类分级要求开展数据分类分级工作。

6.驻场人员要求

供应商应提供不少于1人的驻场运维服务，运维人员对本平台运行维护工作提供全年的7x24小时的保障服务，工作日提供5x8小时的现场保障服务，保证系统稳定运行。驻场运维人员常驻采购人指定办公场地，并通过现场电话、微信等多种方式实现问题处理。

A 包：安全防护项目采购需求

为保障安全防护能力提升项目相关设备安全平稳运行，结合项目实际情况，本项目运维主要包括硬件设备维保，软件维保，运维保障服务、远程技术支持、护网防守服务等。

服务名称	服务范围	服务内容
硬件维保	数据库安全审计工具（安华金和 DAS V3.2 ）1 台 数据库管控防火墙（美创 DF V3.0）2 台 数据库行为防火墙（安华金和 DPS V3.2）2 台 数据库水印工具（安恒 DAS-ABL-AiMask/V2.0）1 台 运维审计堡垒机（奇安信网神 BH/V6.0(C6100-BH-TF30) ）2 台 密码机（奇安信网神 QuickHSM-HS1000 V1.0）2 台	合同签订后提供一年的延保服务，定期开展设备巡检、故障处理、漏洞修复、版本升级、安全设备特征库更新、设备保修及更换配件等
软件维保	数据库加密工具（安华金和 DES V3.2 ）2 套 数据库审计工具（奇安信网神 DAS V6.0 (DAS3000-CLOUD-BIG)）1 套 密码服务套件工具（中安威士 VSEC v3.0）1 套 移动应用安全感知工具（梆梆安全移动应用安全监测软件 V5.0）1 套 Android 应用加固工具（梆梆安全 Android 应用加固软件 V7.0）1 套 小程序加固工具（梆梆安全移动应用加固软件 V7.2（小程序加固））1 套 移动应用安全测评工具（梆梆安全应用安全测评系统 V5.0）1 套 移动应用个人信息隐私合规评估工具（梆梆安全移动应用合规软件 V3.0）1 套 H5 应用加固工具（梆梆安全移动应用加固软件 V7.2	合同签订后提供一年的延保服务，定期开展安全检查、技术咨询、软件授权、软件升级、产品故障处理、漏洞修复等

	（H5 加固））1 套	

1.硬件设备维保

供应商应提供定期设备巡检、故障处理、漏洞修复、版本升级、设备保修及更换配件等。安全设备维保包括但不限于应用识别库、入侵检测特征库、病毒检测特征库等库升级服务、定期设备巡检、故障处理、漏洞修复、版本升级、设备保修及更换配件。

供应商须在采购人故障申报后 30 分钟内完成初步诊断与响应,2 小时内工程师到达现场，48 小时内完成维修或更换。

服务频次：每月至少进行一次设备巡检、检测设备版本，确保设备无异常情况。

交付成果：《巡检报告》。

2.软件维保

供应商应提供定期安全检查、技术咨询、软件升级、产品故障处理、漏洞修复等。

服务频次：每月至少进行一次软件系统检查，内容包括检查系统负载、资源使用率、版本补丁等。

交付成果：《定期检查报告》。

3.运维保障服务

重要特殊时期对软硬件设备的安全状态进行监控，提供专项的安全服务，能在各种异常情况下快速应对，快速处理，使得在重保期间网络系统安全平稳地运行。包括重保前的检查和评估工作、重保中的事中监测、重保后的总结与报告，并及时定位问题，处理问题。

服务频次：重大活动期间/按需。

交付成果：《重保值守安全监测报告》。

4.远程技术支持

远程技术支持人员协助现场人员对重大安全风险、安全事件进行远程支撑分析、安全事件处置闭环、安全处置建议提供等工作。

服务频次：按照采购人需求。

交付成果：《安全事件处置报告》。

5.护网防守服务

配合采购人的护网演习或实战演练安排，做好每年护网前期准备、安全自查整改、攻防演习和演习总结等阶段相关工作。保证护网期间，按要求进行联合作战，充分利用现有软硬件设备的安全防护能力，结合安全监测与分析经验，协助进行实时检测与分析

攻击行为，快速响应处置，抑制攻击事件，顺利完成护网工作。

服务频次：按照采购人需求。

输出：《护网总结报告》。

B包：省一体化政务服务平台（一期）子系统电子证照系统运维项目采购需求

河南省一体化政务服务平台（一期）子系统电子证照系统运维工作应对业务系统、信息资产和安全资产进行全面梳理，形成《系统及功能清单》《系统资产清单》和《安全资产清单》，以资产清单为依托，开展基础环境运维、软件运维工作，以及各业务子系统的信息资源维护、短信发送服务，配合开展信息安全等级测评工作。具体运维需求如下：

1.基础设施运维

1.1 系统巡检与资源监控

对电子证照系统所依赖的服务器、数据库等基础设施开展日常巡检，监控资源使用情况（CPU、内存、磁盘等），发现问题及时处理，确保系统稳定运行。

1.2 资源优化与备份恢复

（1）根据系统运行情况，完成资源优化、扩容、迁移等工作。

（2）制定并执行数据备份策略，确保数据安全可恢复，支持异常数据恢复和系统迁移。

2.系统日常运维

2.1 业务支撑与功能维护

（1）支撑电子证照制发，包括底图配置、目录创建和更新、系统对接（获取制发电子证照所需数据等）、按需回流电子证照等。涉及调用签章能力的，需进行签章功能代码适配改造工作，确保电子证照正常签章。

（2）完成系统模块的日常维护，包括要素录入更新、材料整理、信息资源维护等。

（3）支撑地市及省直单位电子证照数据归集、共享（包括在省大数据平台编目、挂载接口等），解决地市及省直单位关于系统使用的问题，保障日常业务正常开展。

2.2 数据处理与统计分析

（1）按照要求及时、准确提供电子证照统计数据。

（2）定期对电子证照数据上报国家流程进行巡检，保障数据汇聚及时性、数据质检准确性等。

2.3 工单处理与故障响应

（1）处理国家下发的电子证照异议处理和抽检问题、12345热线工单及省政务服务

网、豫事办等渠道收集的异议处理问题。

（2）对系统运行中出现的各类故障进行快速响应和处理，确保业务连续性。

2.4 运维报告与巡检记录

（1）定期开展系统巡检，形成月度、季度、年度运维报告，记录问题处理情况和系统运行状态。

（2）对电子证照格式、文件验章的质检任务进行定期巡检，并对异常情况进行处理。

2.5 保障电子证照系统各组件功能正常发挥，不得以系统组件授权到期、授权数量不足等缘由停止系统服务。

3.数据分类分级

参照《数据安全技术 数据分类分级规则》（GB/T43697—2024）《全国一体化政务大数据体系 政务数据目录 第 3 部分：政务数据分类》（征求意见稿）和河南省一体化政务大数据体系工程标准《政务数据 分类分级指南》完成系统生成数据的分类分级梳理工作，系统汇聚的数据按照行业上级业务指导部门制定的数据分类分级要求开展数据分类分级工作。

4.安全运维

4.1 日常安全监测

组织专业技术力量，依托省级数字政府“一道墙”安全运营支撑平台、电子政务外网态势感知平台和自身监测能力，对省一体化政务服务平台（一期）子系统电子证照系统进行 7×24 小时监测，分析研判系统面临的网络安全攻击，对可能发生的网络安全、数据安全隐患进行处置，确保系统安全稳定运行。

4.2 安全漏洞修复

及时修复网络安全管理、保密管理、密码管理、公安、电子政务、行政审批和政务信息管理等部门通报的安全漏洞。对 CentOS 操作系统采取安全加固措施。及时修复网络安全等级测评、商用密码应用安全性评估、攻防演练、渗透测试、基线核查等发现的安全漏洞。

4.3 重要时期安全保障

按照河南省行政审批和政务信息管理局发布的《重要时期网络安全保障工作指南要求》及每年的重要时期网络安全保障工作提示的重保时间及范围开展重保工作，供应商需根据重保时间及范围制定重保方案，确保方案应科学全面可实施。保障前期各项准备

工作完成，包括前期系统自查整改、系统侧安全设备策略优化、业务调整等内容；保障期间开展现场值班值守、业务运行监测、业务运行播报等内容；根据采购人提供的网络安全系统开展安全告警监测、分析研判、威胁定性与应急响应处置；重保结束后，全面回顾保障期间工作执行情况、安全攻击态势变化、处置成效及经验教训，形成重保总结报告。

4.4 安全合规检查

落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》《互联网政务应用安全管理规定》等法律法规管理制度规定组织开展安全合规检查。按照网络安全管理、保密管理、密码管理、公安、电子政务、行政审批和政务信息管理等部门通报完成安全检查。

4.5 上线前安全自查整改

功能新增或变更上线前，供应商须开展前置性安全自查。自查涵盖以下内容：利用自动化代码审计平台对上线及变更涉及的源代码进行静态分析，检查编码缺陷及安全漏洞；对系统引用的开源组件及第三方库进行成分分析，识别高危漏洞；利用漏洞扫描工具进行自动化检测，协助发现常见的 Web 漏洞和主机漏洞；变更涉及新服务器、新中间件或新数据库环境部署，需对该环境的核心配置项进行自动化核查，识别不符合通用安全基线的配置项。检查结束后出具安全评估报告，对识别出的高风险项提供可行性整改建议，并按照整改建议进行整改，整改后出具复测报告。

4.6 应急演练

定期开展应急演练，提升系统的应急响应能力与防护处置能力。服务期内至少组织开展2次实战模拟演练,重点验证应急响应流程的可行性及各岗位人员的响应联动效率。演练工作包含方案编制、场景模拟与过程记录。演练前需提交《应急演练工作方案》，内容应包含演练目标、演练范围、演练场景设计、参与人员及职责分工、演练流程及时间安排、保障措施及风险控制措施；演练结束后提交《应急演练评估报告》，内容应包含演练过程回顾、演练目标达成情况、预案执行有效性评估、暴露的流程衔接问题与人员能力短板、针对性的预案优化建议及后续改进计划。

4.7 安全体检

服务期内供应商应按系统开展至少 1 次网络安全体检，涵盖资产摸排、脆弱性与合规差距识别。每次体检工作涵盖以下内容：对资产进行全量梳理；对操作系统、数据库及中间件的核心配置项进行自动化检查，识别不符合安全基线规范的配置项；通过模拟

攻击手法对系统进行深度渗透测试，验证系统防御能力的薄弱环节；针对核心业务代码进行源代码缺陷扫描，协助发现编码规范问题。针对检查结果出具专业分析报告，对识别出的高风险项提供可行性整改建议，并视采购人需求配合进行整改后的复测验证。

4.8 其他方面

配合省级数字政府“一道墙”安全运营支撑平台开展安全漏洞扫描，每季度开展一次，共四次,并基于扫描情况完成漏洞整改和反馈工作。完成 AGENT 部署,对于未使用加密网关加密项目,需同步提供出入口 nginx 服务器名单,开通网络策略,一并将监测数据传输到省级数字政府“一道墙”安全运营支撑平台。完成系统资产调研表的反馈及动态更新,按照统一提供的资产调研表模板进行梳理、填写及调整核验工作,确保运维保障系统资产信息的完整性和准确性。组织专业技术人员在国家攻防演练和省级攻防演练期间进行值班值守，发现网络安全攻击及时报告并处置。落实《河南省行政审批和政务信息管理局网络安全事件应急预案》要求，发生安全事件后第一时间组织专业技术人员进行分析研判，及时报告并处置。

5.新老共享交换平台切换

电子证照系统新老共享交换平台切换包括库表数据迁移和共享接口切换两项内容。一是按照新共享交换平台要求，将老共享交换平台上与电子证照有关的库表数据迁移到新共享交换平台，进行目录挂载与订阅、同步流程改造、质检程序修改，并与国家平台对接，确保原有交换任务正常运行。同时，需按照新共享交换平台文件模式，将现有的 FTP 模式进行个性化定制改造。二是将国家平台共享接口、部委共享接口、地市和省直单位共享接口按照新共享平台要求和标准切换,开展接口挂接、订阅及联调测试等工作,确保接口功能正常。

功能新增或变更上线前，供应商须开展前置性安全自查。自查涵盖以下内容：利用自动化代码审计平台对上线及变更涉及的源代码进行静态分析，检查编码缺陷及安全漏洞；对系统引用的开源组件及第三方库进行成分分析，识别高危漏洞；利用漏洞扫描工具进行自动化检测，协助发现常见的 Web 漏洞（如 SQL 注入、XSS 跨站脚本、弱口令等）和主机漏洞（操作系统、数据库、中间件等漏洞）；变更涉及新服务器、新中间件或新数据库环境部署，需对该环境的核心配置项进行自动化核查，识别不符合通用安全基线的配置项。检查结束后出具安全评估报告，对识别出的高风险项提供可行性整改建议，并按照整改建议进行整改，整改后出具复测报告。

6.系统迁移

将现有的电子证照系统迁移至信创云环境中。在系统部署层面，实现系统功能在信创环境部署和证照数据的整体迁移；在系统对接层面，按照国家、省、市三级重新梳理对接清单；最后，在系统完成迁移后，开展适配验证工作，保障信创环境下系统的稳定运行。

7.运维服务时间及人员要求

拟派项目经理1人，项目组成员3人，其中驻场人员不少于2人，提供1年驻场运维服务，。在合同约定服务期内，运维人员对本系统运行维护工作提供全年的7×24小时的保障服务，工作日提供5×8小时的现场保障服务，保证系统稳定运行。驻场运维人员常驻采购人指定办公场地，并通过现场电话、微信等多种方式实现问题处理。

C 包：省一体化协同办公平台运维项目采购需求

本次招标要求中标人为河南省一体化协同办公平台提供全维度、专业化的整体运维服务，服务覆盖日常运维、平台应用推广服务支撑、系统对接三大核心板块，需建立标准化闭环管理体系，组建专属运维团队，制定完善服务方案与应急预案，保障平台 7×24 小时稳定、安全、高效运行，满足全省政务协同办公业务需求，助力政务办公数字化升级。

河南省一体化协同办公平台运维工作应对业务系统、信息资产和安全资产进行全面梳理，形成《系统及功能清单》《系统资产清单》和《安全资产清单》，以资产清单为依托，开展基础环境运维、软件运维工作，以及各业务子系统的信息资源维护，配合开展信息安全等级测评和商用密码应用安全性评估工作。具体要求如下：

1.日常运维服务

日常运维是平台稳定运行的核心保障，中标人需建立标准化、精细化的运维管理体系，配备专业政务运维技术团队，实现不间断保障，做到问题早发现、早响应、早处理，持续优化平台性能，具体包括：

1.1 基础环境及软件运维

安排专人专岗对平台所有的云主机（至少 182 台）及配套的操作系统、数据库、中间件、业务系统开展全维度常态化巡检维护，制定标准化流程与台账。主要运维要求：保障平台 7×24 小时不间断运行，针对基础环境运维保障系统总体可用率不低于 99.9%，日志保存时间不低于 180 天，运维期内无重大故障发生，无重大安全事故发生。

1.1.1 服务器运维内容

服务器日常运维。对新下发的服务器完成操作系统初始化、操作系统优化、操作系统安全加固等工作；对下发的漏洞扫描结果在规定时间内完成服务器漏洞修复，保障高危漏洞 24 小时内完成修复，中危漏洞 3 日内完成修复，漏洞修复较复杂的应在 3 日内制定详尽的漏洞修复方案，报送采购人审批通过后，按照方案执行。

服务器运行监控。对服务器运行状态进行日常监测、对预警问题按照问题处理规范进行问题记录、流转、处理和跟踪等工作，建立健全的系统问题处理机制和规范，对告警日志进行分析研判，精准定性威胁类型（如 SQL 注入、暴力破解等），明确告警等级并执行分级分类处置。建立《攻击告警处置台账》，记录告警来源，研判分析结果、处置情况等。每月提交《月度安全监测分析报告》（含告警总量、Top3 威胁类型、处置

率、未闭环问题说明），保障主机长期处于最优状态。在采购人界定的问题程度下，一般问题 2 个小时解决并记录，较严重问题 4 个小时出具问题解决方案并提交给采购人研判解决。

服务期内供应商应按系统开展至少 1 次网络安全体检，涵盖资产摸排、脆弱性与合规差距识别。每次体检工作涵盖以下内容：对资产进行全量梳理；对操作系统、数据库及中间件的核心配置项进行自动化检查，识别不符合安全基线规范的配置项；通过模拟攻击手法对系统进行深度渗透测试，验证系统防御能力的薄弱环节；针对核心业务代码进行源代码缺陷扫描，协助发现编码规范问题。针对检查结果出具专业分析报告，对识别出的高风险项提供可行性整改建议，并视采购人需求配合进行整改后的复测验证。

服务器资源全生命周期管理。对现有资源进行全面梳理，全面管理资源的申请、调整、释放工作。

1.1.2 中间件运维内容

中间件安装和漏洞修复。根据实际工作要求完成所需中间件的安装、集群搭建、优化、配置、调试和安全加固等工作，开展问题定位排查处理。在采购人界定的问题分类下，一般问题 2 小时内解决，较严重问题 4 小时内出具问题解决方案并提交给采购人研判解决。

中间件运行监控。每日开展中间件的系统监控和问题处理工作，保障中间件长期处于最优状态。

1.1.3 数据库运维内容

数据库安装和漏洞修复。根据实际工作要求配合完成达梦、金仓、Redis、ES 等常用数据库部署、集群的搭建、配置和优化工作；数据库漏洞应在 2 日内编写详细的漏洞修复方案，提报给采购人研判，并按要求完成数据库安全加固和整改，保障数据库的稳定运行。

数据库备份恢复和扩容。按照备份管理要求，对数据库进行备份和巡检。

1.1.4 日常巡检要求内容

做好系统资源日常监控，按政务云要求优化系统资源使用，需进行配置变更时，提供资源变更申请，做好系统资源变更后运行监控。提供每日的操作系统、中间件、数据库、业务系统等运行指标、应用进程运行情况巡检工作，对预警和发现的问题和隐患，提出处理建议或修复方案，并及时处理，一般问题 2 个小时解决，较严重问题协调相关人员 4 个小时出具问题解决方案并提交给采购人研判解决。

1.1.5 运行情况报告内容

月度运维报告。根据业务系统用户量、运行情况和业务办理量等信息，出具业务系统运行报告；对运维工作进行梳理，出具运维月报，月报包括服务器运行情况、中间件运行情况、数据库运行情况等。

季度运维报告。每季度进行系统运行和运维工作总结，提交季度系统运行工作报告，内容包括本季度内的系统运行情况，运维工作情况，需求完成情况，故障及处理情况，安全工作开展情况，其他需要汇报或讨论的内容及下个季度的工作计划等。

年度汇报。每年度进行系统运行和运维工作总结，提交年度系统运行工作报告，内容包括本年内的系统运行情况，运维工作情况，故障处理情况，安全工作开展情况，其他需要汇报或讨论的内容及下个周期工作计划等。

2.安全运维

2.1 日常安全监测

组织专业技术力量，依托省级数字政府“一道墙”安全运营支撑平台、电子政务外网态势感知平台和自身监测能力，对省一体化协同办公平台进行 7×24 小时监测，分析研判系统面临的网络安全攻击，对可能发生的网络安全、数据安全隐患进行处置，确保系统安全稳定运行。

2.2 安全漏洞修复

及时修复网络安全管理、保密管理、密码管理、公安、电子政务、行政审批和政务信息管理等部门通报的安全漏洞。及时修复网络安全等级测评、商用密码应用安全性评估、攻防演练、渗透测试、基线核查等发现的安全漏洞。

2.3 重要时期安全保障

按照河南省行政审批和政务信息管理局发布的《重要时期网络安全保障工作指南要求》及每年的重要时期网络安全保障工作提示的重保时间及范围开展重保工作，供应商需根据重保时间及范围制定重保方案，确保方案应科学全面可实施。保障前期各项准备工作完成，包括前期系统自查整改、系统侧安全设备策略优化、业务调整等内容；保障期间开展现场值班值守、业务运行监测、业务运行播报等内容；根据采购人提供的网络安全系统开展安全告警监测、分析研判、威胁定性与应急响应处置；重保结束后，全面回顾保障期间工作执行情况、安全攻击态势变化、处置成效及经验教训，形成重保总结报告。

2.4 安全合规检查

落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》《互联网政务应用安全管理规定》等法律法规管理制度规定组织开展安全合规检查。按照网络安全管理、保密管理、密码管理、公安、电子政务、行政审批和政务信息管理等部门通报完成安全检查。

2.5 上线前安全自查整改

功能新增或变更上线前，供应商须开展前置性安全自查。自查涵盖以下内容：利用自动化代码审计平台对上线及变更涉及的源代码进行静态分析，检查编码缺陷及安全漏洞；对系统引用的开源组件及第三方库进行成分分析，识别高危漏洞；利用漏洞扫描工具进行自动化检测，协助发现常见的 Web 漏洞和主机漏洞；变更涉及新服务器、新中间件或新数据库环境部署，需对该环境的核心配置项进行自动化核查，识别不符合通用安全基线的配置项。检查结束后出具安全评估报告，对识别出的高风险项提供可行性整改建议，并按照整改建议进行整改，整改后出具复测报告。

2.6 应急演练

定期开展应急演练，提升系统的应急响应能力与防护处置能力。服务期内至少组织开展2次实战模拟演练,重点验证应急响应流程的可行性及各岗位人员的响应联动效率。演练工作包含方案编制、场景模拟与过程记录。演练前需提交《应急演练工作方案》，内容应包含演练目标、演练范围、演练场景设计、参与人员及职责分工、演练流程及时间安排、保障措施及风险控制措施；演练结束后提交《应急演练评估报告》，内容应包含演练过程回顾、演练目标达成情况、预案执行有效性评估、暴露的流程衔接问题与人员能力短板、针对性的预案优化建议及后续改进计划。

2.7 安全体检

服务期内供应商应按系统开展至少 1 次网络安全体检，涵盖资产摸排、脆弱性与合规差距识别。每次体检工作涵盖以下内容：对资产进行全量梳理；对操作系统、数据库及中间件的核心配置项进行自动化检查，识别不符合安全基线规范的配置项；通过模拟攻击手法对系统进行深度渗透测试，验证系统防御能力的薄弱环节；针对核心业务代码进行源代码缺陷扫描，协助发现编码规范问题。针对检查结果出具专业分析报告，对识别出的高风险项提供可行性整改建议，并视采购人需求配合进行整改后的复测验证。

2.8 其他方面

配合省级数字政府“一道墙”安全运营支撑平台开展安全漏洞扫描，每季度开展一次，共四次,并基于扫描情况完成漏洞整改和反馈工作。完成 AGENT 部署,对于未使用加

密网关加密项目,需同步提供出入口 nginx 服务器名单,开通网络策略,一并将监测数据传输到省级数字政府“一道墙”安全运营支撑平台。完成系统资产调研表的反馈及动态更新,按照统一提供的资产调研表模板进行梳理、填写及调整核验工作,确保运维保障系统资产信息的完整性和准确性。组织专业技术人员在国家攻防演练和省级攻防演练期间进行值班值守，发现网络安全攻击及时报告并处置。落实《河南省行政审批和政务信息管理局网络安全事件应急预案》要求，发生安全事件后第一时间组织专业技术人员进行分析研判，及时报告并处置。

3.日常问题处理

中标人对接已使用省一体化协同办公平台的各省直部门，解决用户日常使用反馈的问题。中标人应建立畅通的问题反馈渠道，包括服务热线、在线客服、邮箱等，对用户反馈的 BUG、故障、操作疑问等进行统一记录、分类、编号，建立详细台账。按问题类型制定差异化处理时限：简单操作疑问 1 小时内解答，一般故障 4 小时内启动处理、24 小时内解决，复杂技术问题 2 小时内告知进展、72 小时内解决，特殊情况需提前说明。问题解决后通知用户验证，确保满意度 100%。每周汇总分析问题，每月形成分析报告提交招标单位，从源头减少同类问题发生，形成标准化闭环处理体系。

4.新增需求处理

针对省直部门提出的新增需求，安排专业人员开展需求调研，了解业务背景、功能要求等信息，建立需求管理台账，相关需求收集整理后提交招标单位审批，并配合完成需求的可行性评估。对于招标单位审批通过，具备实施可行性的需求，中标人利用现有业务服务平台技术能力，完成需求模块的搭建、测试。中标人应搭建独立测试环境，相关需求在测试环境搭建测试无误后，更新至生产环境，确保生产环境正常运行；相关需求上线后，需持续监测 1 个月，及时处理问题并提供使用指导。

对于招标单位评估尚不具备实施可行性的需求，中标人应协助提供解决方案，更新完善需求台账，为项目后续规划提供需求依据。

功能新增或变更上线前，供应商须开展前置性安全自查。自查涵盖以下内容：利用自动化代码审计平台对上线及变更涉及的源代码进行静态分析，检查编码缺陷及安全漏洞；对系统引用的开源组件及第三方库进行成分分析，识别高危漏洞；利用漏洞扫描工具进行自动化检测，协助发现常见的 Web 漏洞（如 SQL 注入、XSS 跨站脚本、弱口令等）和主机漏洞（操作系统、数据库、中间件等漏洞）；变更涉及新服务器、新中间件或新数据库环境部署，需对该环境的核心配置项进行自动化核查，识别不符合通用安全基线

的配置项。检查结束后出具安全评估报告，对识别出的高风险项提供可行性整改建议，并按照整改建议进行整改，整改后出具复测报告。

5.配合通过网络安全等级保护测评及商用密码应用安全性评估

在运维服务期间，中标人须配合完成协同办公平台的网络安全等级保护测评及商用密码应用安全性评估工作，按要求提供必要资料与技术支持，并依据测评情况完成相关问题的整改，确保平台通过网络安全等级保护测评及商用密码应用安全性评估，满足合规要求。

6.数据分类分级

参照《数据安全技术 数据分类分级规则》（GB/T43697—2024）《全国一体化政务大数据体系 政务数据目录 第3部分：政务数据分类》（征求意见稿）和河南省一体化政务大数据体系工程标准《政务数据 分类分级指南》完成系统生成数据的分类分级梳理工作，系统汇聚的数据按照行业上级业务指导部门制定的数据分类分级要求开展数据分类分级工作。

7.平台应用推广服务

为扩大平台覆盖范围，实现全省政务协同办公一体化，中标人需为新增接入单位提供全流程一站式应用推广支撑服务，形成标准化上线体系，确保平台平稳落地。

本次平台应用推广服务采购核心要求为：中标人需具备支撑至少100家省直单位推广的能力，为各新增接入省直单位提供一站式、全周期、专业化的推广支撑，建立标准化、可复制的上线体系，确保平台在各省直单位平稳落地、高效运行，保障全省政务协同办公一体化目标顺利实现。投标人应充分分析省直单位在组织架构、人员信息化水平、现有系统使用情况等差异化现状，预判可能存在的接入难点与运行风险，在投标文件中提供详细的平台应用推广服务方案。

中标人需承担省直单位的推广服务工作，全程负责各单位从前期筹备、需求对接、流程搭建到最终上线运维的全流程工作，具体包括：

7.1 需求调研

组建专业调研团队，与新增接入单位深入对接，围绕公文办理、即时通讯、日常办公、业务审批等核心业务，收集表单格式、流程规则、权限分配等具体需求，同时了解单位组织架构、现有系统使用情况。结合平台技术架构制定个性化上线解决方案，调研完成后形成需求调研报告，明确实施步骤与计划，报招标单位及接入单位审核确认，作为后续工作的重要依据。

7.2 流程表单配置

依据审核通过的调研报告，完成流程表单精细化搭建与个性化配置。按需求配置公文、审批表单的字段、校验规则、打印模板，设置流程节点、流转规则与审批权限，结合组织架构完成精细化业务权限配置，同时做好基础数据初始化工作。搭建内部测试环境开展全面测试，验证配置的准确性与流畅性，邀请接入单位内部试用，根据意见完成最终优化，确保符合实际办公需求。

7.3 系统演示优化

平台上线前组织接入单位相关人员制定详细演示方案，结合实际业务案例展示表单填报、流程审批、公文处理等核心功能。安排专业人员现场讲解答疑，记录用户对流程、功能、界面的意见建议，建立反馈台账。完成优化调整，再次组织演示验证，确保平台贴合实际办公需求，提升使用体验。

7.4 人员信息维护

安排专人与接入单位对接，收集审核部门组织架构、用户信息，进行标准化处理后，配合使用部门在平台中完成组织架构创建、用户信息录入工作，并遵循“最小权限”原则，根据用户岗位、职级完成操作、审批、数据查看等权限的精细化配置。后续若发生流程调整、人员变动等情况，配合使用部门管理员完成平台信息更新与权限调整，做好变更记录，确保信息与实际情况保持一致。

7.5 培训

为接入单位全体使用人员开展线上/线下针对性培训，根据人员分布、岗位特点制定个性化培训方案。基础培训覆盖平台登录、系统使用等通用操作，专业培训按岗位划分重点内容，结合实际案例实操讲解。为参训人员发放培训资料与操作手册，同时建立培训档案。

7.6 初期支撑

部门初次上线使用，安排专业人员提供不少于一周的现场或远程全方位支撑，建立快速响应机制。对用户提出的流程微调、权限调整等完成优化，快速处置技术故障，最大限度减少对办公的影响。每日收集用户反馈并优化，支撑结束后形成总结报告，开展使用情况回访，建立常态化服务对接机制，保障后续使用顺畅。

8.系统对接服务

根据业务需求开展平台对外部系统的对接，包括但不限于国家级、省级、市级相关业务系统。中标人需组建专属对接技术团队，提供专业高效的系统对接服务，具体包括：

8.1 第三方应用集成对接

中标人应按照招标单位要求的河南省一体化协同办公平台与第三方应用集成对接规范，配合招标单位开展各省直部门业务应用与省一体化协同办公平台的集成对接工作。第三方应用接入省一体化协同办公平台工作台，中标人组织开展应用系统对接方案沟通研讨，按照河南省一体化协同办公平台与第三方应用集成对接规范要求，了解第三方应用对接需求及系统技术架构，与对接单位共同制定科学可行的对接方案，明确对接需求、对接方式、安全要求及实施计划，报招标单位审核确认。审核通过后，中标人配合第三方应用完成接口对接联调工作，及时解决联调中遇到的问题，保障高效完成系统集成对接工作。

投标人须提供完整可落地的集成对接方案，方案须明确对接方式、对接技术路线、数据格式、安全加密方式及回执反馈机制，确保两系统间身份统一认证、消息互通顺畅，实现业务跨平台协同高效、运行稳定，满足政务办公一体化相关要求。

8.2 公文交换对接

中标人应按照招标单位要求，遵循国家及河南省公文交换标准，配合招标单位完成17个省辖市、济源示范区及航空港区的公文交换对接，推进各省直部门公文交换对接工作。中标人按照招标单位工作安排，配合对接省直部门、各地市政务信息化部门沟通制定针对性对接方案，明确接入方式、接口规范、数据格式、安全加密方式及回执反馈机制，实现公文数据标准化传输与格式转换，做好加密处理保障传输安全。中标人配合开展接口对接及联调测试，解答处理对接过程中遇到的问题，验证公文交换的准确性、及时性与安全性，优化调整功能。建立日常维护机制，确保省一体化协同办公平台公文交换平台运行正常，制定应急处置方案，保障全省公文跨部门、跨区域电子化高效流转。

投标人须提供完整可落地的公文交换对接方案，方案须明确接入方式、对接技术路线、数据格式、安全加密方式及回执反馈机制，实现公文数据标准化传输与格式转换，做好加密处理保障传输安全。

8.3 用户中心对接

中标人应按照河南省一体化协同办公平台用户中心对接规范要求，配合招标单位完成17个省辖市、济源示范区及航空港区的用户中心对接，配合推进各省直部门用户中心对接工作。中标人按招标单位工作安排，配合对接省直部门、各地市政务信息化主管部门，深入沟通双方用户中心系统的信息结构、认证方式等，制定对接方案，明确用户信息同步规则、权限映射关系等信息，实现用户信息实时同步，确保双方系统用户信息

一致。中标人配合开展用户中心接口对接及联调工作，验证信息同步及时性、完整性、准确性，处理解决对接所遇问题。建立日常运维机制，定期巡检系统运行情况和重要时期保障工作。

投标人须提供完整可落地的用户中心对接方案，方案须明确接入方式、对接技术路线、数据格式、安全加密方式及回执反馈机制，明确用户信息同步规则、权限映射关系等信息，实现用户信息实时同步，确保双方系统用户信息一致。

9.项目实施要求

9.1.团队要求。

中标人需组建专属项目服务团队，项目经理 1 人，常驻服务人员数量不少于 5 人，岗位覆盖系统运维、安全防护、业务支撑、技术对接等核心工作，明确各岗位职责与资质要求。核心人员需经招标方面试确认，合同期内不得随意更换，确需更换需提前 15 个工作日书面申请并经同意。同时，根据平台应用推广与系统对接的实际推进节奏，中标人需在常驻服务人员基础上按需增加相应人员，确保各阶段工作衔接顺畅、人力配置充分满足项目推进需求。

9.2. 服务报告与沟通机制。

建立常态化汇报机制，按要求输出运维工作周报、月报、季报，清晰反馈平台运行状态、工作开展情况、问题处理结果、后续工作计划等内容，由招标方对服务成效进行评估。

9.3. 文档管理。

规范运维过程管理，对所有工作环节形成完整的过程文档，包括但不限于巡检记录、问题处理台账、需求调研资料、系统配置文档、对接测试报告、培训资料等，确保运维工作可追溯、可核查。

9.4. 保密管理。

制定完善的团队保密管理制度与实操措施，明确团队成员保密责任、操作规范及违规追责条款，定期开展内部保密培训与自查，主动配合招标方开展团队保密措施的定期评估与不定期核查，按要求提交保密工作相关材料。

9.5. 考核机制。

制定完善的服务承诺、服务水平体系、服务管理等相关实施措施，搭建层级清晰的服务水平体系，明确关键指标。建立标准化、规范化的服务管理机制，接受招标方全流程监督与考核。考核结果与服务费用支付挂钩，连续两季度不达标的，招标方有权启动

退出机制。

D包 ：省电子政务外网管理中心（一期）运维项目采购需求

河南省电子政务外网管理中心（一期）（以下简称“网管中心（一期）”）是河南省电子政务外网的重要组成部分，主要包括硬件设备135台和软件5套，部署在中原大数据中心（河南省郑州市郑东新区白沙镇杨桥大道252号）。上联国家电子政务外网，下联17个省辖市及济源示范区和航空港区，横向连接省政务云和省直厅局委办。

1.运维需求内容

为保障全省电子政务外网安全平稳运行，结合项目实际情况，网管中心（一期）运维项目主要采购需求包括硬件设备维保，软件维保，运维保障服务等。详见下表：

服务名称	服务范围		服务内容
硬件维保	服务器	华为2288H V5 7台 H3C R4900 G3 2台	合同签订后提供一年的原厂延保服务。服务器、网络设备、分光器的设备维保包括定期设备巡检、故障处理、漏洞修复、版本升级、设备保修及配件更换等。安全设备维保包括安全设备的应用识别库、入侵检测特征库、病毒检测特征库等库升级服务、定期设备巡检、故障处理、漏洞修复、版本升级、设备保修及更换配件。
	网络设备	华为NE40E-X16A 2台 华为NetEngine AR6280 10台 华为NetEngine AR6140 40台 华为S6730-S24X6Q 2台 华为S5735-L24T4S-A 4台	
	安全设备	迪普DPX17000-A12 2台 迪普异常流量监测1台 迪普异常流量清洗1台 ZDNS （万兆）v3.0 2台 华为UMA1550E 2台 华为USG6525E 4台 亚信SpiderFlow-10000 3台 奇安信NGSOC-NDS9000-TZ15M 2台 奇安信NGSOC-NDS9000-TX 25 1台 流量可视化检测采集设备科来RAS9000 1台	

服务名称	服务范围		服务内容
	其他	国产分光器 35 个 IT 机柜 14 架	
软件维保	网管软件	RIIL IT 监控管理系统 V6.8 安全管理平台 1 套 科来网络流量分析审计系统 V7.0 1 套	合同签订后提供一年的原厂延保服务，定期开展版本检查、软件授权、软件升级、产品故障处理、漏洞修复等，并提供技术咨询服务。
	安全软件	亚信安全监测综合分析和业务支撑系统 1 套 亚信网络防病毒软件（服务器版）1 套 迪普综合安全网关集中管理系统 1 套	
运维保障服务	常态化运维保障服务	配备驻场工程师 4 人	日常安全运维服务、驻场服务、值班值守、网络性能监测及故障处理、信息资源维护、安全监控、IP 封禁（互联网、政务外网）等工作。
	重保期运维保障服务	另配备驻场工程师 2 人	重保期间运维保障服务、应急演练支撑服务、护网防守服务。

2.服务具体内容

2.1 硬件设备维保

网管中心（一期）硬件设备共包括服务器设备 9 台、网络设备 58 台、安全设备 19 台、分光器 35 个、IT 机柜 14 架。服务器、网络设备、分光器的设备维保包括定期设备巡检、故障处理、漏洞修复、版本升级、设备保修及配件更换等。安全设备维保包括安全设备的应用识别库、入侵检测特征库、病毒检测特征库等库升级服务、定期设备巡检、故障处理、漏洞修复、版本升级、设备保修及更换配件。

其中设备巡检要求每月至少进行一次设备巡检，并对设备版本同步检测，确保设备无异常情况；故障处理、漏洞修复、版本升级按需开展；设备保修及配件更换要求服务期内对损坏的设备零部件、板卡等进行免费保修或更换，要求针对核心设备（包括华为NE40E-X16A 2 台、迪普 DPX17000-A12 2 台）零部件、板卡等故障申报后 30 分钟内完成初步诊断与响应，2 小时内工程师到达现场，48 小时内完成维修或更换，核心设备外的硬件设备零部件、板卡等故障申报后 60 分钟内完成初步诊断与响应，4 小时内工程师到达现场，4 个工作日内完成维修或更换；安全设备的应用识别库、入侵检测特征库、病毒检测特征库等应在官方发布最新版本后 24 小时内升级完成。

2.2 软件维保

网管中心（一期）共有产品软件 5 套，包括网管软件 1 套，流量可视化系统 1 套；安全监测综合分析和业务支撑系统 1 套，网络防病毒软件（服务器版）1 套，综合安全网关集中管理系统 1 套。软件维保包括定期检查、技术咨询、软件升级、产品故障处理、漏洞修复等。

其中，定期检查要求每月至少进行一次软件系统检查，内容包括检查系统负载、资源使用率、版本补丁等；技术咨询、软件升级、产品故障处理、漏洞修复等按需开展。

3.运维保障服务

3.1 日常运维服务

服务提供方按照要求派遣工程师至指定场地开展长期驻场服务，开展 7×24 小时值班值守，负责网络性能监测、故障处理、网络策略优化、软件补丁与更新、变更支持、网络巡检、接听并处理省电子政务外网接入单位报障或咨询电话等日常运维工作。

运维人员要定期输出以下交付物：《值班日志》，频率：每天；《河南省省级电子政务外网运行周报》《河南省省级电子政务外网运行月报》《河南省省级电子政务外网运行年报》（其中软硬件维保的巡检情况，应在月报中体现），频率：周报/每周、月报/每月、年报/每一年；《事件处置跟踪表》，频率：按需。

3.2 信息资源维护

维护更新网管中心的网络拓扑图、IP 地址、业务流程、资产，识别资产属性，进行资产应用识别、资产攻击面分析、资产变更分析、资产异常连接分析，发现资产异常行为，建立资产台账。

输出交付物：《资产台账表》《资产变更管理表》，频率：按需。

3.3 安全防护

供应商基于采购人提供的安全系统及资产范围，通过态势感知系统等安全软件按要求对安全威胁进行安全监控，处理安全告警，对来自互联网、电子政务外网的安全威胁进行处置。

对告警日志进行分析研判，精准定性威胁类型（如 SQL 注入、暴力破解等），明确告警等级并执行分级分类处置。建立《攻击告警处置台账》，记录告警来源，研判分析结果、处置情况等。每月提交《月度安全监测分析报告》（含告警总量、Top3 威胁类型、处置率、未闭环问题说明）。

服务期内供应商应按系统开展至少 1 次网络安全体检，涵盖资产摸排、脆弱性与合规差距识别。每次体检工作涵盖以下内容：对资产进行全量梳理；对操作系统、数据库及中间件的核心配置项进行自动化检查，识别不符合安全基线规范的配置项；通过模拟攻击手法对系统进行深度渗透测试，验证系统防御能力的薄弱环节；针对核心业务代码进行源代码缺陷扫描，协助发现编码规范问题。针对检查结果出具专业分析报告，对识别出的高风险项提供可行性整改建议，并视采购人需求配合进行整改后的复测验证。

输出交付物：《安全威胁处置表》、《月度安全监测分析报告》

频率：按月。

3.4 重保期间运维保障服务

在满足重要时期总体网络安全保障的要求下，重要特殊时期对省政务外网的安全状态进行监控，通过明确的职责分工与协作，提供专项的安全服务，能在各种异常情况下快速应对，快速处理，确保在重保期间网络系统安全平稳地运行。包括重保前，完成保障前期各项准备工作，包括前期系统自查整改、系统侧安全设备策略优化、业务调整等的检查和评估工作，重保中开展现场值班值守、业务运行监测、业务运行播报等内容；根据采购人提供的网络安全系统开展安全告警监测、分析研判、威胁定性与应急响应处置等，重保后全面回顾保障期间工作执行情况、安全攻击态势变化、处置成效及经验教训，及时定位问题，处理问题并形成重保总结报告。

输出交付物：《重保值守安全监测报告》，频率：重大活动期间/按需。

3.5 应急演练支撑服务

供应商协助采购人完善网络安全应急协调机制，依据现有网络架构修订或完善应急响应预案。供应商应协同采购人开展电子政务外网相关的应急演练，通过模拟应急事件重点验证应急响应流程的可行性和锻炼工作人员的实际处理能力，检验应急处理人员对应急事件、应急处理相关制度掌握情况，验证应急处置方案的有效性与可行性。加强对

突发安全事件的紧急处理能力，根据可能面临的主要风险和系统特点，检验应急处理流程及突发安全事件的处理能力。

演练前需提交《应急演练工作方案》，内容应包含演练目标、演练范围、演练场景设计、参与人员及职责分工、演练流程及时间安排、保障措施及风险控制措施；演练结束后提交《应急演练评估报告》，内容应包含演练过程回顾、演练目标达成情况、预案执行有效性评估、暴露的流程衔接问题与人员能力短板、针对性的预案优化建议及后续改进计划。

输出交付物：《应急演练评估报告》，频率：按需。

3.6 护网防守服务

供应商协助采购人完善网络安全应急协调机制，依据现有网络架构修订或完善应急响应预案。服务期内至少组织开展一次实战模拟演练，重点验证应急响应流程的可行性及各岗位人员的响应联动效率。演练工作包含方案编制、场景模拟与过程记录。做好每年攻防演练期间的前期准备、安全自查整改、正式攻防演习和演习总结等阶段相关工作。演练前需提交《应急演练工作方案》，内容应包含演练目标、演练范围、演练场景设计、参与人员及职责分工、演练流程及时间安排、保障措施及风险控制措施；演练结束后提交《应急演练评估报告》，内容应包含演练过程回顾、演练目标达成情况、预案执行有效性评估、暴露的流程衔接问题与人员能力短板、针对性的预案优化建议及后续改进计划。保证护网期间，按要求进行联合作战，充分利用现有安全检测与防御手段，结合安全监测与分析经验，协助进行实时检测与分析攻击行为，快速响应处置，抑制攻击事件，顺利完成护网工作。

输出交付物：《攻防演练报告》，频率：按需。

3.7 数据分类分级

参照《数据安全技术 数据分类分级规则》（GB/T43697—2024）《全国一体化政务大数据体系 政务数据目录 第 3 部分：政务数据分类》（征求意见稿）和河南省一体化政务大数据体系工程标准《政务数据 分类分级指南》完成系统生成数据的分类分级梳理工作，系统汇聚的数据按照行业上级业务指导部门制定的数据分类分级要求开展数据分类分级工作。

输出交付物：《数据分级分类清单》，频率：按需。

4.服务场地要求

本项目设备部署在中原大数据中心，驻场服务人员需在中原大数据中心进行现场值班值守办公。

4.1 服务方式要求

要求服务提供方进行 7×24 小时不间断现场服务。服务提供方需要为值班人员配备专用值班电话至少一台，服务提供方需为驻场人员按照中原大数据中心统一着装要求自行购置着装，服务提供方需为每位驻场人员配备一台办公电脑。

4.2 服务响应时限要求

针对网管中心各级故障，服务提供方需在规定时限内响应和抢修，具体要求如下：

故障级别	故障内容	故障响应时限	故障抢修时限
一级故障	网管中心省级核心节点主备设备全阻，影响全网核心业务运行历时≥10 分钟；综合安全网关设备全阻，影响访问政务云等业务历时≥15 分钟	3 分钟	0.5 小时
二级故障	网管中心运维区主备防火墙或主备交换机全阻，影响网管中心运维业务历时≥60 分钟；网管软件故障，影响监测业务历时≥60 分钟；省级核心节点设备、综合安全网关半阻，业务单设备运转，影响主备部署架构历时≥60 分钟；为用户单位配置的接入路由器故障，影响用户访问政务外网历时≥60 分钟；DNS 设备故障，影响政务外网公用网络区地址解析历时≥60 分钟	5 分钟	1 小时
三级故障	网管中心运维区单设备故障，业务单设备运转，影响主备部署架构历时≥60 分钟	10 分钟	2 小时
四级故障	其他一般故障	15 分钟	4 小时

4.3 人员要求

服务提供方提供除项目经理（可不驻场）外不少于 4 人的常驻场服务人员团队，常驻人员必须专职为本项目提供服务，重要保障期等特殊时期增加配备驻场工程师至少 2 人。

项目经理应具备丰富的信息化运维项目管理经验、网络和安全服务经验，熟悉运维服务流程，掌握网络及相关安全技术，熟悉主流网络设备、安全设备、服务器等，能够开展日常网络配置、网络快速排障、安全溯源、安全处置等工作。识别指出工作流程中的问题与不足、制定完善安全管理制度、分析优化安全技术措施，协调各方做好安全运维服务，定期向采购人汇报运维工作情况。要求项目经理须具有计算机技术与软件专业技术资格（水平）考试信息系统项目管理师证书，同时具有计算机技术与软件专业技术资格（水平）考试网络工程师或网络规划设计师证书。

其他驻场工程师应具备一定的运维工作经验，熟练掌握路由器、交换机、防火墙的操作技能、熟悉网络监测、网络故障排查处理、安全监测、安全分析等工作，能够根据工作计划开展日常运维保障，承担及时发现威胁、评估风险、应急响应和值班值守等任务。要求每位驻场工程师具有计算机技术与软件专业技术资格（水平）考试中级及以上证书、或中级及以上职称证书、或中国信息安全测评中心颁发的注册信息安全专业人员证书。

项目驻场工程师具备坚定的政治立场，拥有良好的服务意识和思想道德品质，做事勤恳，能吃苦耐劳；遵守国家及省相关法律法规、采购人规章制度，遵守中原大数据中心相关管理规定，服从采购人工作安排。

E包 ：局属信息系统网络安全等级保护测评项目采购需求

1.系统清单

序号	局属信息系统分项名称	等保等级
1	河南省省级一体化政务服务平台	三级
2	河南省政务服务移动端“豫事办”(一期)	三级
3	河南省“豫正通”	三级
4	河南省电子政务外网管理中心（一期）	三级
5	河南省“互联网+监管”系统（一期）	三级
6	河南省一体化协同办公平台	三级
7	河南省大数据中心(一期)	三级

2.总体要求

按照《信息安全等级保护管理办法》（公通字〔2007〕43号）、《信息系统安全等级保护实施指南》（信安字〔2007〕10号）和《信息安全等级保护安全建设 整改工作指导意见》（公信安〔2009〕1429号）（含附件）等公安部信息安全等级保护系列文件要求，对系统清单中的局属信息系统开展网络安全等级保护测评，具体信息安全技术标准以文件相应部分提及的为准，国家标准和国际标准不一致的地方则参照国家标准。

2.1 需遵循的政策法规

（1）《中华人民共和国网络安全法》（2017年6月1日正式实施）

（2）《中华人民共和国保守国家秘密法》（1988年9月5日中华人民共和国主席令第6号公布）

（3）《中华人民共和国保守国家秘密法实施办法》（国家保密局文件国保发〔1990〕1号）

（4）《中华人民共和国国家安全法》（主席令68号，1993年2月22日第七届全国人民代表大会常务委员会第三十次会议通过）

（5）《中华人民共和国计算机信息系统安全保护条例》（国务院令147号）

（6）《计算机信息系统保密管理暂行规定》(国家保密局文件国保发〔1998〕1号）

（7）《计算机信息系统国际联网保密管理规定》(国家保密局文件国保发[1999]1号）

（8）《中华人民共和国计算机信息网络国际联网管理暂行规定》（国务院令195号）

（9）《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》（1997年12月8日国务院信息化工作领导小组审定）

（10）《计算机病毒防治管理办法》（2000年4月26日中华人民共和国公安部第51号令）

（11）《计算机信息网络国际联网安全保护管理办法》（1997年12月11日国务院批准，1997年12月30日公安部发布）

（12）《计算机信息系统安全专用产品分类原则》（1997年4月公安部发布）

（13）《互联网电子公告服务管理规定》（信息产业部2000年10月8日第4次部务会议通过）

（14）《计算机信息系统安全等级保护划分准则》（GB/T17859-1999）

（15）《计算机信息系统安全等级保护网络技术要求》（GA/T387-2002）

（16）《计算机信息系统安全等级保护操作系统技术要求》（GA/T388-2002）

（17）《计算机信息系统安全等级保护数据库管理系统技术要求》（GA/T389-2002）

（18）《计算机信息系统安全保护等级划分准则》（1999年9月国家技术监督局发布）

（19）《计算机信息系统安全等级保护通用技术要求》（GA/T390-2002）

（20）《计算机信息系统安全等级保护管理要求》（GA/T391-2002）

（21）《计算机机房场地安全要求》（GB9361-88）投标人必须遵循但不限于以上法律法规。

2.2 行业规范

《信息安全等级保护管理办法》(公通字[2007]43 号)

(1) 《信息安全技术 网络安全等级保护实施指南》(GB/T 25058-2019)

(2) 《信息安全等级保护安全建设整改工作指导意见》(公信安[2009]1429 号)(含附件)

(3) 《信息安全技术 网络安全等级保护定级指南》（GA/T 1389-2017）

(4) 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

(5) 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

(6) 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）

3.服务内容

按照信息安全等级测评2.0标准对采购人指定信息系统进行等保测评，供应商现场测评结束后，汇总测评数据，出具整改方案，并协助指导整改工作。供应商根据测评的内容和结果出具相应的等级保护测评报告，并完成在公安部门的备案工作。提供信息安全咨询服务；7×24小时网络安全应急支撑服务，必要时 2 小时内到达现场。

3.1 等级测评内容

本项目按照信息安全等级保护测评标准进行安全等级测评。测评内容主要包括两个方面：一是单元测评，测评指标与《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）相应等级的基本要求完全一致；二是系统整体测评，主要测评分析信息系统的整体安全性。

单元测评包括安全技术测评和安全管理测评两大部分，其中安全技术测评层面主要包含：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心。安全管理测评层面主要包含：安全管理制度、安全管理人员、安全管理机构、安全建设管理、安全运维管理。

整体测评在单元测评的基础上进行进一步测评分析，在内容上主要包括安全控制间、层面间和区域间相互作用的安全测评以及系统结构的安全测评等。

(1) 安全物理环境：主要包含物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护 10 个方面的内容。

(2) 安全通信网络：主要包含网络架构、通信传输、可信验证 3 个方面的内容。

(3) 安全区域边界：主要包含边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等 6 个方面的内容。

(4) 安全计算环境：主要包含身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护 11 方面的内容。

(5) 安全管理中心：主要包含系统管理、审计管理、安全管理、集中管控 4 个方面的内容。

(6) 安全管理制度：主要包含岗位设置、人员配备、授权和审批、沟通和合作、审核和检查 5 个方面的内容。

(7) 安全管理人员：主要包含人员录用、人员离岗、安全意识教育和培训、外部人员访问管理4个方面的内容。

(8)　安全管理制度：主要包含岗位设置、人员配备、授权和审批、沟通和合作、审核和检查 5 个方面的内容。

(9)　安全建设管理：主要包含定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务投标人选择 10 个方面的内容。

（10）安全运维管理：主要包含环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理 14 个方面的内容。

系统整体测评涉及到信息系统的整体拓扑、局部结构，也关系到信息系统的具体安全功能实现和安全控制配置，与特定信息系统的实际情况紧密相关，内容复杂且充满系统个性。因此，全面地给出系统整体测评要求的完整内容、具体实施方法和明确的结果判定方法是很困难的。测评人员应根据特定信息系统的具体情况，结合本标准要求，确定系统整体测评的具体内容，在安全控制测评的基础上，重点考虑安全控制间、层面间以及区域间的相互关联关系，测评安全控制间、层面间和区域间是否存在安全功能上的增强、补充和削弱作用以及信息系统整体结构安全性、不同信息系统之间整体安全性等。

3.2 测评具体要求

在安全等级测评过程中，每个工作阶段、流程、内容及成果交付严格遵循《信息安全技术 网络安全等级保护测评要求》GB/T28448-2019 和《信息安全技术 网络安全等级保护测评过程指南》GB/T28449-2018 文件，根据本项目信息系统已完成的定级备案安全等级，开展相应级别的安全等级测评工作，根据测评结果出具相应的单项和整体测评报告，测评报告需得到项目单位的确认，并报送网安部门审核、批复。测评报告编制的内容及格式严格遵照《网络安全等级保护测评报告模版（最新版）》进行。

测评技术团队符合《网络安全等级测评与检测评估机构自律规范》对测评机构和测评人员的管理要求，项目负责人由公安部培训考核认证通过的信息安全高级等级测评师承担，通过注册信息安全专业认证、具备良好的教育背景、受过专业的技术培训、拥有丰富的行业信息安全及等级测评安全服务工作经验，对用户在信息系统安全等级测评过程中可能会面临的各类技术问题提供及时解决方案。

3.3 测评交付成果

项目阶段各阶段的测评过程文档（参照《信息安全技术信息系统安全等级保护测评

过程指南》）编制。详见下表（包括但不限于）：

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

4.安全整改

依据采购人信息系统安全等级测评的相关报告，编制并提交相关的信息安全整改建议方案，并全程协助完成整改工作。

4.1 具体要求

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

4.2 过程文档及交付成果

过程文档及交付成果（包括但不限于）要求如下：

安全等级测评实施方案、安全等级测评整改技术方案、安全等级测评报告等，可根据整改和规划内容的重要性和复杂程度采用分册方式编写。

提交要求：涉及所有被测评系统的安全整改方案，需包含如下内容：

方案分项	详细内容及要求

等级化安全保障建议方案	内容应包括但不限于以下方面： 1、安全区域和等级划分； 2、安全体系框架设计； 3、等级化安全指标体系报告。
安全体系建设建议方案	内容应包括但不限于以下方面： 1、网络面临风险分析； 2、针对性措施建议。
相关网络安全管理制度	内容应包括但不限于以下方面： 1、机房安全管理制度； 2、网络故障应急预案及应急方案流程制度； 3、客户端管理制度； 4、数据备份及恢复制度； 5、灾难恢复策略及制度。

5. 人员要求：

拟派项目经理 1 人，项目组成员 9 人其中包含渗透测试人员 1 人和技术人员 8 人，人员具有 3 年以上从事信息系统安全等级测评服务工作经验。

6.验收评价

采购人将对供应商的项目交付成果进行评价，供应商应根据采购人的评价意见对项目交付成果进行修改。

当因供应商原因严重影响采购人业务系统正常运转，采购人对交付结果有否决权。

7.服务要求

鉴于测评工作实施的复杂性，投标人必须逐条予以明确以下承诺：

（1）在测评过程中，当与其它应用系统（含硬件、集成平台、应用系统、数据库系统等）发生任何矛盾时（如协作冲突、技术分歧等），均应服从采购人的协调或裁决。

（2）供应商实行项目总负责人制，在项目验收前，供应商不得随意更换；如确需更换，需事先向采购人提交书面更换意见函，征得采购人同意答复后进行更换。

（3）项目实施过程中，由采购人召集的现场协调会，通知供应商项目总负责人、各子系统技术负责人到场的，供应商项目总负责人、各子系统技术负责人必须到场，进行

沟通、协调及裁决，并形成书面备忘录，项目总负责人签字并执行，不得以任何理由推诿。

售后服务要求：

供应商必须对售后服务，做出详细的实质性承诺，包括售后服务免费技术支持期、服务响应速度、服务模式、售后服务质量控制、客户化培训等。所有的售后费用，必须计入投标总价。

（1）售后服务免费技术支持期1年，提供7×24小时远程服务,必要时2小时内到达现场提供紧急情况的应急支持服务，确保在8小时内解决问题；

（2）服务期内按采购人需求提供协助整改服务；

（3）客户培训（提供网络安全培训服务，服务期内制定培训计划，不少于2次对采购人进行安全意识教育、等级保护等安全基础知识培训）。

F包：局属信息系统密码应用安全性评估项目采购需求

1.系统清单

序号	局属信息系统分项名称	等保等级
1	河南省“豫正通”	三级
2	河南省大数据中心(一期)	三级
3	河南省一体化协同办公平台	三级

2.总体要求

依据GB/T 39786-2021《信息系统密码应用基本要求》、GB/T 43206-2023 《信息安全技术 信息系统密码应用测评要求》、GM/T 0116-2021《信息系统密码应用测评过程指南》、《信息系统高风险判定指引》和系统自身的安全需求分析，对被评估系统进行商用密码应用安全性评估，为被测系统的商用密码安全提供科学评价，逐步规范网络运营者的密码使用和管理行为。在商用密码应用安全性评估完成后，提交《商用密码应用安全性评估报告》到当地密码管理局和采购人。

2.1 实施方式

系统评估，及时发现系统脆弱性，识别变化的风险，了解系统安全状况。对照密码应用方案对系统开展评估。根据被评估对象的实际情况、所属行业及系统使用的密码产品情况，选择并确定测评依据。在系统真实环境下进行测评，以评估密码保障是否安全有效，密码使用是否合规、正确、有效。并通过测评发现系统存在的安全隐患和风险，提出可行性完善建议。

2.2 需遵循的政策法规及行业规范：

1、依据标准

信息系统密码安全服务全过程所有工作严格按照最新国家相关安全标准执行，以保证服务工作科学、规范地进行，具体参考的标准如下：

《GB/T 39786-2021信息系统密码应用基本要求》

《GB/T 43206-2023 信息安全技术 信息系统密码应用测评要求》

《GM/T 0116-2021信息系统密码应用测评过程指南》

《商用密码应用安全性评估管理办法》

《信息系统密码应用高风险判定指引》

《政务信息系统密码应用与安全性评估工作指南》2020版

《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知（国办发〔2019〕57号）》

《国家密码管理局关于请进一步加强国家政务信息系统密码应用与安全性评估工作的函（国密局函〔2020〕119号）》。

3.服务内容

3.1 评估内容

商用密码应用安全性评估时按照相关要求分别从系统技术和安全管理等方面全方位对信息系统的密码使用情况进行评估，评估范围主要包括：物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密码算法、密码技术、密码产品、密码服务、安全管理相关文档等，主要具体内容如下表：

序号	评估内容		评估对象
1	通用要求	密码算法测评	密码算法
		密码技术测评	密码技术
		密码产品测评	密码产品
		密码服务测评	密码服务
2	物理和环境安全测评	身份鉴别	物理机房
		电子门禁记录数据完整性	物理机房
		视频记录数据完整性	物理机房
		密码服务	物理机房
		密码产品	物理机房
3	网络和通信安全测评	身份鉴别	网络链路
		通信数据完整性	网络链路
		通信数据机密性	网络链路
		访问控制信息完整性	网络链路
		接入设备的真实性	网络链路
		密码服务	网络链路

序号	评估内容		评估对象
		密码产品	网络链路
4	设备和计算安全测评	身份鉴别	密码设备、数据库、服务器
		远程管理通道安全	密码设备、数据库、服务器
		访问控制信息完整性	密码设备、数据库、服务器
		重要信息资源安全标记完整性	密码设备、数据库、服务器
		日志记录完整性	密码设备、数据库、服务器
		重要可执行程序完整性	密码设备、数据库、服务器
		密码服务	密码设备、数据库、服务器
		密码产品	密码设备、数据库、服务器
5	应用和数据安全测评	身份鉴别	应用
		访问控制信息完整性	应用
		重要信息资源安全标记完整性	应用
		重要数据传输机密性	应用
		重要数据存储机密性	应用
		重要数据传输完整性	应用
		重要数据存储完整性	应用
		不可否认性	应用
		密码服务	应用
		密码产品	应用
6	安全管理测评	管理制度	安全管理相关文档
		人员管理	安全管理相关文档
		建设运行	安全管理相关文档
		应急处置	安全管理相关文档

3.2 通用要求评估

密码算法测评

测评单元	测评指标	测评方式
密码算法合规性检查	信息系统中使用的密码算法应当符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。	访谈、文档审查和实地查看或配置检查
		文档审查和实地查看或配置检查

密码技术测评

测评单元	测评指标	测评方式
密码技术合规性检查	信息系统中使用的密码技术应遵循密码相关国家标准和行业标准。	访谈、文档审查和实地查看或配置检查

密码产品测评

测评单元	测评指标	测评方式
密码产品合规性检查	信息系统中使用的密码产品与密码模块应通过国家密码管理部门核准。	访谈、文档审查和实地查看或配置检查

密码服务测评

测评单元	测评指标	测评方式
密码服务合规性检查	信息系统中使用的密码服务应通过国家密码管理部门许可。	访谈、文档审查和实地查看或配置检查

3.3 物理和环境安全测评

测评单元	测评指标	测评方式
身份鉴别	8.1 a）宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；	访谈和文档审查
		文档审查和实地查看或配置检查
		至少包括配置检查或工具测试中的一种
电子门禁记录数据完整性	8.1 b）宜采用密码技术保证电子门禁系统进出记录数据的存储完	访谈和文档审查
		文档审查和实地查看或配置

测评单元	测评指标	测评方式
	整性；	检查
		至少包括配置检查或工具测试中的一种
视频记录数据完整性	8.1 c）宜采用密码技术保证视频监控音像记录数据的存储完整性。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		至少包括配置检查或工具测试中的一种
密码服务	8.2 f）以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		至少包括配置检查或工具测试中的一种
密码产品	8.2 g）以上采用的密码产品，应达到GB/T 37092 二级及以上安全要求。	访谈和文档审查
		访谈、文档审查和实地查看或配置检查
		访谈、文档审查和实地查看或配置检查

3.4 网络和通信安全测评

测评单元	测评指标	测评方式
身份鉴别	8.2 a）应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		访谈、文档审查和实地查看或配置检查
通信数据完整性	8.2 b）宜采用密码技术保证通信过程中数据的完整性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种

测评单元	测评指标	测评方式
		文档审查和实地查看或配置检查
重要数据的机密性	8.2 c）应采用密码技术保证通信过程中重要数据的机密性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
网络边界访问控制信息的完整性	8.2 d）宜采用密码技术保证网络边界访问控制信息的完整性；	文档审查，同时，至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
安全接入认证	8.2 e）可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
密码服务	8.2 f）以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
密码产品	8.2 g）以上采用的密码产品，应达到GB/T 37092 二级及以上安全要求。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查

3.5 设备和计算安全测评

测评单元	测评指标	测评方式
身份鉴别	8.3 a）应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
远程管理通道安全	8.3 b）远程管理设备时，应采用密码技术建立安全的信息传输通道；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
访问控制信息完整性	8.3 c）宜采用密码技术保证系统资源访问控制信息的完整性；	文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
重要信息资源安全标记完整性	8.3 d）宜采用密码技术保证设备中的重要信息资源安全标记的完整性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
日志记录完整性	8.3 e）宜采用密码技术保证日志记录的完整性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
重要可执行程序完整性、重要可执行程序来源真实性	8.3 f）宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。	访谈和文档审查
		至少包括配置检查或工具测试中的一种

测评单元	测评指标	测评方式
		文档审查和实地查看或配置检查
密码服务	8.3 g）以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查
密码产品	8.3 h）以上采用的密码产品，应达到GB/T 37092 二级及以上安全要求。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
		文档审查和实地查看或配置检查

3.6 应用和数据安全测评

测评单元	测评指标	测评方式
身份鉴别	8.4 a）应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种，并结合文档审查
访问控制信息完整性	8.4 b）宜采用密码技术保证信息系统应用的访问控制信息的完整性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种，并结合文档审查
重要信息资源安全标记完整性	8.4 c）宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
重要数据传输机密性	8.4 d）应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
重要数据存储机密性	8.4 e）应采用密码技术保证信息系统应用的重要数据在存储过程	访谈和文档审查
		至少包括配置检查或工

测评单元	测评指标	测评方式
	中的机密性；	具测试中的一种
重要数据传输完整性	8.4 f）宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；	访谈和文档审查
		至少包括配置检查或工具测试中的一种
重要数据存储完整性	8.4 g）宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；	访谈、文档审查和现场查看
		至少包括配置检查或工具测试中的一种，并结合文档审查
不可否认性	8.4 h）在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
密码服务	8.4 i）以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。	访谈和文档审查
		至少包括配置检查或工具测试中的一种
密码产品	8.4 j）以上采用的密码产品，应达到GB/T 37092 二级及以上安全要求。	访谈和文档审查
		至少包括配置检查或工具测试中的一种

3.7 安全管理测评

测评单元		测评指标	测评方式
管理制度	具备密码应用安全管理制度	8.5 a）应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；	访谈、文档记录核查。
	密钥管理规则	8.5 b）应根据密码应用方案建立相	访谈、文档记录核

测评单元		测评指标	测评方式
		应密钥管理规则；	查。
	建立操作规程	8.5 c）应对管理人员或操作人员执行的日常管理操作建立操作规程；	访谈、文档记录核查。
	定期修订安全管理制度	8.5 d）应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定,对存在不足或需要改进之处进行修订；	访谈、文档记录核查。
	明确管理制度发布流程	8.5 e）应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；	访谈、文档记录核查。
	制度执行过程记录留存	8.5 f）应具有密码应用操作规程的相关执行记录并妥善保存。	访谈、文档记录核查。
人员管理	了解并遵守密码相关法律法规 和密码管理制度	8.6 a）相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；	访谈、文档记录核查。
	建立密码应用岗位责任制度	8.6 b）应建立密码应用岗位责任制度,明确各岗位在安全系统中的职责和权限： 1）根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位； 2）对关键岗位建立多人共管机制； 3）密钥管理、密码安全审计、密码操作人员职责互相制约互相监督,其中密钥管理员岗位不可与密码审计员、密码操作员等关键安全岗位兼任；	访谈、文档记录核查。

测评单元		测评指标	测评方式
		4) 相关设备与系统的管理和使用账号不得多人共用。	
	建立上岗人员培训制度	8.6 c) 应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；	访谈、文档记录核查。
	定期进行安全岗位人员考核	8.6 d) 应定期对密码应用安全岗位人员进行考核；	访谈、文档记录核查。
	建立关键岗位人员保密制度和调离制度	8.6 e) 应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。	访谈、文档记录核查。
建设运行	制定密码应用方案	8.7 a）应依据密码相关标准和密码应用需求，制定密码应用方案；	访谈、文档记录核查。
	制定密钥安全管理策略	8.7 b）应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节，各环节安全管理要求参照《信息安全技术 信息系统密码应用基本要求》附录A；	访谈、文档记录核查。
	制定实施方案	8.7 c）应按照应用方案实施建设；	访谈、文档记录核查。
	投入运行前进行商用密码应用安全性评估	8.7 d）投入运行前应进行商用密码应用安全性评估，评估通过后系统方可正式运行；	访谈、文档记录核查。
	定期开展商用密码应用安全性评估及攻防对抗演习	8.7 e）在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展商用密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。	访谈、文档记录核查。
应急	应急策略	8.8 a）应制定密码应用应急策略，	访谈、文档记录核

测评单元		测评指标	测评方式
处置		做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置；	查。
	事件处置	8.8 b）事件发生后，应及时向信息系统主管部门进行报告；	访谈、文档记录核查。
	向有关主管部门上报处置情况	8.8 c）事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。	访谈、文档记录核查。

4.安全整改

依据采购人信息系统商用密码应用安全性评估的相关报告，编制并提交相关的信息安全整改建议方案，并采取相应的措施全程协助完成整改工作，以提高密码的安全性和可靠性。

4.1 具体要求

4.1.1 评估现有密码策略：对现有的密码策略进行评估，包括密码的复杂度、长度、更换周期等，以及密码的管理流程和安全意识培训等。

4.1.2 发现存在的问题和漏洞：通过测试和检查等手段，发现密码设置、使用和管理中存在的问题和漏洞，如弱密码、密码泄露、密码管理不规范等。

4.1.3 分析问题原因：对发现的问题进行深入分析，找出问题的根本原因，如人员安全意识不足、技术手段落后、管理密码评估整改是指对密码的设置、使用和管理进行评估，发现存在的问题和漏洞，并采取相应的措施进行整改，以提高密码的安全性和可靠性。

4.1.4 制定整改方案：根据问题原因，制定相应的整改方案，包括加强密码管理、提升安全意识、更新技术手段等。

4.1.5 实施整改措施：按照整改方案，采取具体的措施进行整改，如加强密码复杂度要求、开展安全意识培训、更新密码管理工具等。

4.1.6 验证整改效果：对整改后的密码策略进行再次评估和测试，验证整改效果是否符合预期，如未达到预期效果，则需进一步调整整改方案。

4.2 过程文档及交付成果

过程文档及交付成果（包括但不限于）要求如下：

商用密码应用安全性评估实施方案、商用密码应用安全性评估整改技术方案、商用密码应用安全性评估报告等。

5. 人员要求：

（1）项目经理1人且具有商用密码应用安全性评估8年以上工作经验。

（2）拟派技术负责人1人且有商用密码应用安全性评估5年以上工作经验。

（3）拟派项目组技术人员4人且具有商用密码应用安全性评估3年以上工作经验。

6.验收评价

采购人将对供应商的项目交付成果进行评价，供应商应根据采购人的评价意见对项目交付成果进行修改。

当因供应商原因严重影响采购人业务系统正常运转，采购人对交付结果有否决权。

7.服务要求

供应商必须对售后服务，做出详细的实质性承诺：售后服务免费技术支持期、服务响应速度、服务模式、售后服务质量控制等。所有的售后费用，必须计入投标总价。

（1）售后服务免费技术支持期1年，提供7×24小时远程服务,必要时2小时内到达现场提供紧急情况的应急支持服务，确保在8小时内解决问题；

（2）服务期内按采购人需求提供协助整改服务。

（3）技术咨询培训（提供密码应用安全咨询服务，服务期内制定技术咨询计划）。

G 包：局属信息系统综合安全监管项目采购需求

依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》及网络安全等级保护 2.0 标准要求，通过常态化、全流程的综合安全监管服务，全面识别省一体化政务服务平台（一期）、“豫事办”（一期）、省“豫正通”、省“互联网+监管”系统（一期）、省一体化协同办公平台、省电子政务外网管理中心（一期）、安全防护项目和内容安全监测项目等属政务信息系统存在的安全漏洞与风险隐患，开展常态化渗透测试、新增功能上线前安全检查、安全审计、风险评估、安全漏洞复测、专项安全检查、安全咨询、安全培训等，提升系统整体安全防护能力，保障政务数据安全和业务稳定运行。

1.常态化渗透测试服务

供应商在授权和监督下，对指定的局属政务信息系统进行受控的、非破坏性的渗透测试，目的是侵入系统，获取系统控制权并将入侵的过程和细节生成报告给用户，由此证实用户系统所存在的安全威胁和风险，测试范围覆盖 Web 应用、操作系统、数据库、中间件、网络设备、API 接口、身份认证与权限控制及业务逻辑等各个层面，重点排查敏感数据泄露、越权访问、SQL 注入、XSS 跨站脚本、CSRF 跨站请求伪造、文件上传漏洞、命令执行等高危风险，对发现的漏洞进行利用验证和危害程度分析，并针对安全隐患提出解决办法，切实保证信息系统安全。加固后进行复测，检验安全加固效果。

供应商须提供适配采购人场景的自动化渗透测试解决方案，应具备自动化漏洞检测能力，以便快速识别系统潜在风险。需同时提供服务工具的功能界面截图，并加盖生产厂商公章作为技术能力证明。

服务频次：按采购人需求提供服务，服务期内不少于 4 次。

交付成果：《XX 系统渗透测试报告》（含漏洞详情、危害等级、影响范围、验证过程、整改建议等内容）。

2.上线前安全检查服务

供应商应对采购人提供拟上线的新系统、新模块、新功能进行上线前安全检测，根据系统上线要求开展基线核查、漏洞扫描、代码审计、开源组件检查、部署环境评估等安全检测，全面提升信息系统上线前的整体防护水平，保障信息系统上线后的整体安全性。针对发现的安全问题，给出整改建议并进行全程跟踪验证，确保所有高危及以上漏洞整改完成后方可上线。

供应商须自带基线检查、漏洞扫描、代码审计、开源组件检测服务工具，使用检测

工具需为自主研发，具备完整知识产权。禁止使用开源免费工具、社区版工具、二次开发改造工具或无资质第三方工具。

服务频次：按采购人需求提供服务，每次新增功能/系统上线前完成。

交付成果：《XX 系统上线前安全评估报告》、《上线安全评估意见书》（明确是否具备上线条件）

3.安全审计服务

供应商利用服务工具对信息系统、网络、数据、应用、管理制度及运维操作进行全面检查、合规校验、风险识别、行为追溯、闭环整改等，用于保障系统合规、数据安全、业务稳定，满足等保、数据安全法等监管要求，服务内容包括但不限于安全制度与合规性审计、网络与业务系统安全审计、数据安全审计、安全运维与管理审计等。

供应商须自带服务工具，服务工具需为自主研发，具备完整知识产权。禁止使用开源免费工具、社区版工具、二次开发改造工具或无资质第三方工具。

服务频次：按采购人需求提供服务，服务期内不少于 4 次。

交付成果：《XX 系统安全审计报告》、《合规性评估报告》、《风险清单与整改建议》

4.风险评估服务

供应商应采用定性与定量相结合的方法，对局属政务信息系统进行全面的安全风险评估，系统识别资产价值、威胁来源和脆弱点，科学分析安全事件发生的可能性和影响程度，准确计算风险等级并划分风险优先级。在安全管理体系评估中，不仅要评估安全策略、规章制度、程序、表单体系的完整性，而且会评估这些制度是否得到贯彻执行，是否及时更新，是否全面覆盖需进行信息安全风险评估的信息系统。在安全技术体系评估中，对信息系统面临的安全风险进行识别与分析，采用传统的风险评估方法，从资产、威胁、脆弱性的角度，对前端业务处理接口安全，业务数据传输安全、服务端的物理、网络、系统、应用、数据等层面的安全，进行风险值量化。制定包括风险规避、风险降低、风险转移和风险接受在内的风险处置方案，同时评估现有安全防护措施的有效性并提出针对性的安全加固建议。

供应商须按照《信息安全技术 信息安全风险评估方法》（GB/T20984-2022） 国标标准对局属政务信息系统现有网络架构、安全设备、安全策略、业务系统访问控制等进行详细的安全检查和测试评估，评估技术漏洞、管理漏洞及物理漏洞等，找出安全薄弱点，并协助整改。

服务频次：按采购人需求提供服务，服务期内不少于 1 次。

交付成果：《网络安全风险评估报告》、《数据安全风险评估报告》

5.安全漏洞复测服务

供应商应对所有采购人发现的漏洞进行整改后的复测验证，确认整改措施的有效性和漏洞的完全修复状态，对未完全修复或修复不彻底的漏洞提供进一步的整改建议，同时对整改过程中可能引入的新漏洞进行检测，建立并维护完整的漏洞整改闭环管理机制。

供应商须自带服务工具，服务工具需为自主研发，具备完整知识产权。禁止使用开源免费工具、社区版工具、二次开发改造工具或无资质第三方工具。

服务频次：按采购人需求提供服务，服务期内每个局属政务信息系统不少于 2 次

交付成果：《漏洞复测报告》（每次复测后提交）

6.专项安全检查服务

供应商应针对特定安全主题或重要时期开展专项安全检查，常规检查主题包括勒索病毒防护、重大活动保障检查、数据安全、移动应用安全、云平台安全、供应链安全及重大活动安全保障等，检查内容根据专项主题确定并重点排查该领域存在的突出安全问题，同时提供专项安全加固建议和针对性的应急处置预案。

供应商须提供全年的安全检查支持服务，包括现场检查、远程支持、问题复测等方面的服务。

服务频次：按采购人需求提供服务，服务期内不少于 2 次。突发安全事件立即开展针对性专项检查，不受服务频次限定。

交付成果：《XX 专项安全检查报告》

7.安全应急响应服务

供应商应根据所涉及的资产清单，结合局属政务信息系统部署环境，建立健全应急管理机制，编制完善应急预案，组织开展应急演练，验证预案有效性。梳理数据风险、网络攻击等场景处置流程。对于系统突发紧急故障，在接到通知后第一时间做出响应，开展专业的应急响应工作，并提交相应的问题处理方案、应急材料供采购人研判。故障处理完毕后出具故障分析报告，确保突发安全事件有效处置，保障业务连续性。

供应商须在接到采购人通知后 2 小时内采取相应措施以确保系统正常运行。无法在 2 小时内解决的，须在采购人要求时间内提交。

服务频次：按采购人需求提供服务，服务期内不限次数。

交付成果：《XX 系统网络和数据安全应急预案》

8.安全咨询服务

供应商应根据采购人需要，提供 7×24 小时电话和在线安全咨询服务，及时解答日常安全问题，协助制定和完善安全管理制度、应急预案及操作流程，提供安全事件应急响应咨询和技术支持，给出安全设备选型、部署和配置建议，持续跟踪国内外最新安全动态、漏洞信息和攻击手段并及时发布安全预警，同时协助开展等级保护测评、关键信息基础设施认定等合规性工作。

供应商须提供全年的安全检查支持服务，包括现场检查、远程支持、问题复测等方面的服务。

服务频次：按采购人需求提供服务，服务期内不限次数。

交付成果：安全服务月报（每月提供）、安全相关参考文件等。

9.网络安全风险威胁情报收集

供应商应根据采购人需要，采集多源异构威胁情报，包括但不限于 IP 信誉情报（支持 IPv4、IPv6，含威胁类型、严重级别、地理位置等标签）、IOC 失陷情报（支持 IP 及域名查询，可识别标注攻击团伙）、漏洞威胁情报（支持通过漏洞编号、名称等多维度查询）；同时整合开源情报、第三方商业情报及局属系统内部安全日志、网络流量等数据，确保情报来源全面、内容详实。对采集的原始情报进行清洗、去重、关联分析及人工研判，剔除无效、重复数据，确保情报准确性和可操作性。

每周向采购人提交一份标准化情报报告，明确威胁等级、影响范围、潜在风险及初步处置建议

服务频次：按采购人需求提供服务，服务期内不限次数。

交付成果：网络安全风险威胁情报报告。

10.驻场人员要求

供应商应提供不少于 6 人的驻场安全服务，其中项目经理、技术负责人、技术人员须符合技术配备相关要求。

驻场人员须工作日常驻采购人指定办公场地，提供 5x8 小时的现场安全服务，并通过电话、微信等多种方式，提供 7x24 小时的远程安全服务实现问题处置。

第六章 投标文件格式

河南省行政审批和政务信息管理局2026年度局属政务信息系统运维项目

投 标 文 件

采购编号：

投标人（企业电子签章）：_____

法定代表人或其委托代理人：_____（签字或盖章）

_____年_____月__日

目　录

一、开标一览表

金额单位：元人民币

投标人名称	
项目名称	
包名称	
投标报价	大写：_____元 小写：_____元 **注：投标人所报价格包括了完成本项目所发生的所有费用。**
服务周期	
服务地点	
合同履行期限	
投标范围	
投标有效期	自投标截止时间之日起 90 日历天
其他声明	

投标人（企业电子签章）：_____

法定代表人或授权代表人（签字或签章）：_____

日期：　　年　　月　　日

二、投标函

致（采购人）：_____

我方收到了贵单位采购编号为_____的_____（项目名称） 包招标文件，经研究，我公司决定参加该项目的投标活动，并按要求提交投标文件。我们郑重声明以下内容并负法律责任：

根据贵方的投标邀请,我方签字代表(姓名、职务)经正式授权，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）愿按照招标文件中规定的条款和要求，提供完成招标文件规定的全部工作，投标总报价为(大写)_____元人民币(RMB￥：_____元)，合同履行期限为_____，维保期为_____。

（2）本投标有效期为自投标截止之日起 90 个日历天。

（3）联合体中的大中型企业和其他自然人、法人或者非法人组织，与联合体中的小型、微型企业之间_____(存在、不存在）投资关系（若投标人为联合体）。

（4）已详细审查全部招标文件，包括所有补充文件、更正公告、澄清、答疑文件（如有），完全理解并同意放弃对这方面有不明、误解的权利。

（5）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，我方与采购代理机构不存在附属关系。

（6）若我方中标，同意按招标文件的规定的收费标准和方式，一次性支付招标代理服务费。

（7）按照贵方可能的要求，提供与投标有关的一切真实数据或资料，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。

（8）按照招标文件的规定履行合同责任和义务。

（9）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。

（10）与本次投标有关的一切正式往来请寄：

地址：_____

投标人（企业电子签章）：_____

法定代表人或授权代表人（签字或签章）：_____

日期：　　年　　月　　日

三、法定代表人身份证明及授权委托书

（一）法定代表人身份证明

单位名称：_____

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_____（投标人单位名称）的法定代表人。

特此证明。

附：身份证扫描件（反、正面）

投标人（企业电子签章）：_____

日　　期：_____年_____月_____日

（二）法定代表人授权委托书

本授权委托书声明：我_____（姓名）系_____（投标人名称）_____的法定代表人，现授权委托的_____（姓名）为我公司代理人，代理人根据授权，以我方名义签署、澄清、说明、补正、递交、撤回、修改_____（项目名称）_包_的投标文件，以及签订合同和处理有关事宜，其法律后果由我方承担。

本授权书于_____年_____月_____日签字生效,特此声明。

附：法定代表人身份证扫描件

附：代理人身份证身份证扫描件

投标人（企业电子签章）：_____

法定代表人（签字或签章）：_____

委托代理人（签字或签章）：_____

日　　期：　　年　　月　　日

四、投标人资格证明文件

（一）法人或者非法人组织的营业执照等证明文件

说明：营业执照/《社会团体法人登记证书》/《民办非企业单位登记证书》。

（二）承诺书

我公司郑重声明：

我公司符合 河南省行政审批和政务信息管理局2026年度局属政务信息系统运维项目（项目编号：_____）招标文件规定的资格条件，依法缴纳税收和社会保障金，且无纳税、社保等方面失信记录，具备履行合同所必需的设备和专业技术能力，符合法律、行政法规规定的其他条件。

若我公司声明或承诺不属实，同意取消本项目的参与资格，并将承担相关法律责任，接受处理。

投标人（企业电子签章）：_____

法定代表人或授权代表人（签字或签章）：_____

日　　期：　　年　　月　　日

（三）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声明函

我公司承诺：

我公司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，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，同意取消本项目的参与资格，并将承担相关法律责任，接受处理。

投标人（企业电子签章）：_____

法定代表人或授权代表人（签字或签章）：_____

日　　期：　　年　　月　　日

（四）反商业贿赂承诺书

我公司承诺：在_____投标活动中，保证做到以下几点承诺：

一、公平竞争参加本次招投标活动。

二、杜绝任何形式的商业贿赂行为。不向国家工作人员、采购人、采购代理机构工作人员、评审专家或其亲属提供礼品、礼金、有价证券、购物券、回扣、佣金、咨询费、赞助费、宣传费、宴请等；不为其报销各种消费凭证，不支付其旅游、娱乐等费用。

三、若违反上述承诺，我公司及参加与投标的工作人员愿意接受按照法律法规有关规定接受相应处罚。

投标人（企业电子签章）：_____

法定代表人或授权代表人（签字或签章）：_____

日　　期：　　年　　月　　日

（五）2024 年度或 2025 年度财务状况报告或银行资信证明

（六）2025 年 9 月 1 日以来任意一个缴纳税收和社会保障资金的相关材料

（七）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，不得参加同一标包投标或未划分标包的同一招标项目投标（投标人自行承诺）

五、分项报价表

（一）分项报价表说明

可针对报价范围等方面进行说明。

（二）分项报价表

单位：人民币元

序号	名称	数量	单价	总价	备注

投标人（企业电子签章）：_____

法定代表人或授权代表人（签字或签章）：_____

日　　期：　　年　　月　　日

六、类似业绩

序号	项目名称	实施时间	实施单位

投标人（企业电子签章）：_____

法定代表人或授权代表人（签字或签章）：_____

日　　期：　　年　　月　　日

七、服务方案及计划

投标人可根据评审标准等要求自行提供。

八、人员配备状况

（一）拟派主要人员汇总表

序号	本项目任职	姓名	职称	执业或职业资格证明			备注
				证书名称	级别	证号	

投标人（企业电子签章）：_____

法定代表人或授权代表人（签字或签章）：_____

日　　期：　　年　　月　　日

（二）主要人员简历表

姓　名		年龄		执业资格证书（或上岗证书）名称	
职　称		学历		拟在本项目任职	
工作年限				从事本行业工作年限	
毕业学校	年毕业于　　学校　　专业				
主要工作经历					
时　间	参加过的类似项目			担任职务	委托人及联系电话

注：项目负责人应附身份证、学历证（如有）、职称证（如有）、注册执业资格证书（如有）或上岗证书（如有）、社保缴费证明复印件，管理过的项目业绩（如有）须附合同协议书复印件等相关证明材料。主要人员附身份证、学历证（如有）、职称证（如有）、有关证书（如有）和社保缴费证明复印件等相关证明材料。

投标人（企业电子签章）：_____

法定代表人或授权代表人（签字或签章）：_____

日　　期：　　年　　月　　日

（三）人员安排及管理制

九、投标人提供产品适用政府采购政策情况表

（如有）

（一）强制采购通过相关认证的清单产品(如有)

投标产品中强制采购通过节能认证的产品					
序号	货物名称	规格型号	生产厂商	证书编号	备注
1					
2					
….	…. .	….	….	…. .	
投标产品中强制采购经国家认证的信息安全产品					
序号	货物名称	规格型号	生产厂商	证书编号	备注
1					
2					
….	…. .	….	….	…. .	
投标产品中强制采购通过3C认证的产品					
1					
2					
….	…. .	….	….	…. .	

说明：

1.如采购人所采购产品为《关于印发节能产品政府采购品目清单的通知》财库〔2019〕19号“节能产品政府采购品目清单”中政府强制采购节能产品的（标记“★”产品），投标人应提供有效期内的节能认证证书（认证机构：应符合《市场监管总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告》[2019年第16号]的“参与实施政府采购节能产品认证机构名录”），否则其投标将被认定为投标无效。

2.如采购人所采购产品属于信息安全产品的，根据《关于信息安全产品实施政府采购的通知》财库[2010]48号和国家质量监督检验检疫总局、国家认证认可监督管理委员会《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号的规定，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。

3.投标产品已列入《市场监管总局关于优化强制性产品认证目录的公告》【2020年第18号】的产品必须提供通过国家3C认证的有关证明材料。否则其投标将被认定为投标无效。

（二）政府采购优先采购的清单产品（如有）

投标产品中通过节能认证的产品								
序号	货物名称	规格型号	生产厂商	证书编号	单价	数量	合计	备注
1								
2								
….	…. .	….	….	…. .				
投标产品中通过环境标志认证的产品								
1								
2								
….	…. .	….	….	…. .				
投标产品中无线局域网产品								
1								
2								
….	…. .	….	….	…. .				

说明：

1.对于投标产品属于“节能清单”中非标记“★”产品并经“机构名录”中的认证机构出具相应的产品认证证书的给于优先采购体现（详见评标标准）。

2.采购人采购产品属于节能产品或环境标志产品品目清单范围内,且投标人所投产品具有有效期内的环境标志产品认证证书，在评标时予以优先采购，具体优惠措施为：如果采购项目包有多种设备,在技术部分打分项中给于优先采购体现(详见评标标准)。

3.投标人所投产品列入“财政部国家发展改革委信息产业部关于印发无线局域网产品政府采购实施意见的通知财库［2005］366号”无线局域网产品清单的，在评标时予以优先采购，具体优惠措施为：如果采购项目包有多种设备，在技术部分打分项中给于优先采购体现（详见评标标准）。

十、投标人企业（单位）类型声明函

（提醒：如果供应商不是中小企业，则不需要提供《中小企业声明函》。否则，因此导致虚假投标的后果由供应商自行承担。）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，服务全部由符合政策要求的中小企业承接。相关企业（含联合 体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1.（标的名称），属于（采购文件中明确的所属行业）；承接企业为（企业名称），从业人员___人，营业收入为____万元，资产总额为 ____万元，属于（中型企业、小型企业、微型企业）；

2.（标的名称），属于（采购文件中明确的所属行业）；承接企业为（企业名称），从业人员___人，营业收入为____万元，资产总额为__万元，属于（中型企业、小型企业、微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（企业电子章）：

日期：

注：1.属于中小微企业的填写此声明函，不属于的无须附此表。2.供应商出具的中小企业声明函不属于采购标的所属行业 或 标的未包含招标文件所列的全部标的，可以不认可其中小企业资格，但不能以此为由否决其参加投标的资格。

（提醒：中小企业对其声明内容的真实性负责，声明函内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。）

1、从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新企业可不填报。

2、中标人如为小型和微型企业的，随中标结果公开中标人的《中小企业声明函》。投

标供应商提供声明函内容不实的，属于提供虚假材料谋取中标。

3、根据《关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19 号）规定，对符合本办法规定的小微企业报价给予 10%的扣除，用扣除后的价格参与评审。

（二）残疾人福利性单位声明函（若有）

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）：_____

法定代表人或授权代表人（签字或签章）：_____

日　　期：　　年　　月　　日

注：

1、在政府采购活动中，残疾人福利性单位视同小型、微型企业；

2、属于残疾人福利性单位的填写，不属于的无需填写此项内容。

（三）投标人监狱企业声明函（若有）

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）服务。

（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。

法定代表人或授权代表人（签字或签章）：_____

日　　期：　　年　　月　　日

十一、投标人认为有必要提供的其他资料

包括但不限于以下内容：

1、项目组人员组成情况（格式自拟）

2、符合采购需求要求的相关服务承诺。

3、……