河南省教育考试院

信息系统安全服务项目

竞争性磋商文件

项目编号：豫财磋商采购-2025-747

采购人：河南省教育考试院

采购代理机构：河南省国贸招标有限公司

二〇二五年七月

特 别 提 示

1.供应商注册

供应商应首先办理CA数字证书及电子签章（具体办理事宜请查询河南省公共资源交易中心网站-公共服务-办事指南）；方能完成市场主体信息库入库登记（具体办理事宜请查询河南省公共资源交易中心网站-公共服务-办事指南）；市场主体信息库入库登记通过后，凭CA数字证书登陆市场主体系统，按网上提示下载招标文件及资料（详见 https://hnsggzyjy.henan.gov.cn//公共服务-办事指南《新交易平台使用手册（培训资料）》。

2.投标文件制作

2.1 供应商通过“河南省公共资源交易中心（https://hnsggzyjy.henan.gov.cn//）”网站公共服务（办事指南《新交易平台使用手册（培训资料）》及下载专区）：下载“投标文件制作工具安装包压缩文件下载”等。

2.2 供应商凭CA密钥登陆市场主体并按网上提示自行下载项目所含格式(.hnzf)的招标文件。

2.3 供应商须在投标文件递交截止时间前制作并提交：加密的电子投标文件（*.hntf 格式），应在投标文件截止时间前通过“河南省公共资源交易中心（https://hnsggzyjy.henan.gov.cn//）”电子交易平台内上传；

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

2.5 供应商在制作电子投标文件完成后须加盖电子签章或公章（包括企业电子签章或公章、个人电子签章或签名）。

2.6 本次招标采用“远程不见面”开标方式，供应商无需到现场参加开标会议。供应商应当在投标截止时间前,登录不见面开标大厅（https://hnsggzyjy.henan.gov.cn//）,在线准时参加开标活动并进行文件解密、答疑澄清、磋商、最后报价等（详见 https://hnsggzyjy.henan.gov.cn//新交易平台使用手册（培训资料）河南省公共资源“智慧交易”平台-不见面开标大厅供应商操作手册），未在规定时间内解密的投标文件将被拒绝。

2.7 供应商编制投标文件时，涉及营业执照、资质、业绩、获奖、人员、财务、社保、纳税、各类证书等内容，必须在市场主体信息库中已登记的信息中选取。提供的具体内容及要求按招标文件相应评审因素提供。

供应商利用投标文件制作工具制作投标文件时，评审资料部分是从主体信息库相应菜单中已录入内容进行挑选，之后形成信息表，同时获取对应扫描件进行展示。

2.8 招标文件格式所要求包含的全部资料应全部制作在投标文件内，严格按照本项目招标文件所有格式如实填写（不涉及的内容除外），不应存在漏项或缺项，否则将存在投标文件被拒绝的风险。

2.9 投标文件以外的任何资料采购人和采购代理机构将拒收。

2.10 供应商编辑电子投标文件时，根据招标文件要求用法人CA密钥和企业CA密钥进行签章制作；最后一步生成电子投标文件（*.hntf格式和*.nhntf格式）时，只能用本单位的企业CA密钥。

2.11 未尽事宜请仔细阅读河南省公共资源交易平台相关操作手册或说明。

3.澄清与变更

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

4.因河南省公共资源交易中心平台在开标前具有保密性，供应商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，因供应商未及时查看而造成的后果自行承担。

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 竞争性磋商公告

项目概况

河南省教育考试院信息系统安全服务项目的潜在供应商应在河南省公共资源交易中心（http://hnsggzyjy.henan.gov.cn/）获取采购文件，并于 2025 年 8 月 5 日 9 时 00 分（北京时间）前递交响应文件。

一、项目基本情况

1、项目编号：豫财磋商采购-2025-747

2、项目名称：河南省教育考试院信息系统安全服务项目

3、采购方式：竞争性磋商

4、预算金额：人民币 3600000.00 元

最高限价：人民币 3600000.00 元

序号	包号	包名称	包预算（元）	包最高限价（元）
1	豫政采(2)20251198-1	河南省教育考试院信息系统安全服务项目	3600000.00	3600000.00

5、采购需求：

5.1 采购内容：河南省教育考试院全院网络安全服务内容主要包括采购方各项招生考试业务信息系统的等级保护测评，全院所有网络设备、安全设备、服务器及终端的日常安全巡检、定期漏洞扫描，各项招生考试业务信息系统上线前的源代码安全检测，各项招生考试业务信息系统的定期漏洞扫描、风险评估、渗透测试及安全加固，日常办公运维、内网安全态势监测与分析、互联网暴露面安全监测与分析、重点业务安全保障、专项安全治理、网络攻防演习、安全管理人员的专业技能培训和全院办公人员的安全技术及意识培训等，囊括采购方动态的、整体的安全管理和保障体系的建立。

5.2 服务期限：自合同签订之日起 36 个月。

5.3 服务地点：采购人指定地点。

5.4 质量要求：符合国家及相关行业规定及采购人要求。

6、合同履行期限：合同签订起至本项目结束。

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、申请人的资格要求

1、满足《中华人民共和国政府采购法》第二十二条规定。

2、落实政府采购政策需满足的资格要求：无。

3、本项目的特定资格要求：

3.1 具有公安部第三研究所颁发的有效的《网络安全等级测评与检测评估机构服务认证证书》。

3.2 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名单、重大税收违法失信主体名单、政府采购严重违法失信行为记录名单的供应商，拒绝参与本项目政府采购活动。[查询渠道：“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）]。

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

三、获取采购文件

1.时间：2025 年 7 月 23 日至 2025 年 7 月 29 日，每天上午 00:00 至 12:00，下午 12:00 至 23:59。

2.地点：河南省公共资源交易中心（https://hnsggzyjy.henan.gov.cn/）

3.方式：登录“河南省公共资源交易中心”，凭企业身份认证锁（CA 数字证书）按网上提示下载获取磋商文件，供应商未按规定在“河南省公共资源交易中心”网站上下载磋商文件的，其响应将被拒绝。供应商需要完成信息登记及 CA 数字证书办理，才能通过河南省公共资源交易平台参与交易活动。具体办理事宜请查阅河南省公共资源交易中心网站“办事指南”专区的《新交易平台使用手册（培训资料）》。

4.售价：0 元

四、响应文件提交

1.时间：加密电子响应文件递交/上传截止时间（响应截止时间，下同）为 2025 年 8 月 5 日 9：00（北京时间）

2.地点：加密电子响应文件须在响应截止时间前通过“河南省公共资源交易中心（https://hnsggzyjy.henan.gov.cn/）”电子交易平台中递交/上传，加密电子响应文件逾期或未按规定递交/上传的，采购人不予受理。

五、响应文件开启

1、时间：2025 年 8 月 5 日 9:00（北京时间）

2、地点：河南省公共资源交易中心远程开标室(六)-6，郑州市经二路 12 号（经二路与纬四路向南 50 米路西）。

六、发布公告的媒介及公告期限

本次采购公告在《河南省政府采购网》、《河南省公共资源交易中心网站》上发布，公告期限为三个工作日。

七、其他补充事宜

1.执行节能、环保、中小企业优惠、监狱企业、残疾人福利企业等政府采购政策，具体政府采购政策落实情况详见采购文件。

2.本项目采用“远程不见面”开标方式，供应商无需到河南省公共资源交易中心现场参加磋商会议。供应商应当在响应截止时间前，登录不见面开标大厅（https://hnsggzyjy.henan.gov.cn//），在线准时参加开标活动并进行文件解密、答疑澄清、磋商、最后报价等（详见 https://hnsggzyjy.henan.gov.cn//新交易平台使用手册（培训资料）河南省公共资源“智慧交易”平台-不见面开标大厅供应商操作手册）。

3.本项目代理服务费由中标（成交）人依据《河南省招标代理服务收费指导意见》豫招协【2023】002 号有关规定向采购代理机构交纳。

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：河南省教育考试院

地址：郑州市郑东新区熊耳河路 1 号

联系人：宋涛

联系方式：0371-68101634

2、采购代理机构信息

名称：河南省国贸招标有限公司

地址：郑州市农业路 72 号国际企业中心 B 座三楼东侧

联系人：常宗义　刘江

联系方式：0371-69136959

E-mail：hngmzb3@163.com

3、项目联系方式

项目联系人：常宗义　刘江

联系方式：0371-69136959

第二章 供应商须知

供应商须知前附表

条款号	条款名称	编列内容
1.2.1	采购人	名称：河南省教育考试院 地址：郑州市郑东新区熊耳河路 1 号 联系人：宋涛 联系方式：0371-68101634
1.2.2	采购代理机构	采购代理机构：河南省国贸招标有限公司 地　址：郑州市农业路 72 号国际企业中心 B 座三楼东侧 联 系 人：常宗义　刘江 联系电话：0371—69136959 传　　真：0371—69131088 邮　　箱：hngmzb3@163.com
1.3.1	项目名称	河南省教育考试院信息系统安全服务项目
1.3.2	项目编号	豫财磋商采购-2025-747
1.3.3	采购内容	河南省教育考试院全院网络安全服务内容主要包括采购方各项招生考试业务信息系统的等级保护测评，全院所有网络设备、安全设备、服务器及终端的日常安全巡检、定期漏洞扫描，各项招生考试业务信息系统上线前的源代码安全检测，各项招生考试业务信息系统的定期漏洞扫描、风险评估、渗透测试及安全加固，日常办公运维、内网安全态势监测与分析、互联网暴露面安全监测与分析、重点业务安全保障、专项安全治理、网络攻防演习、安全管理人员的专业技能培训和全院办公人员的安全技术及意识培训等，囊括采购方动态的、整体的安全管理和保障体系的建立。
1.3.4	服务期限	自合同签订之日起 36 个月。

1.3.5	合同履行期限	合同签订起至本项目结束。
1.3.6	质量要求	符合国家及相关行业规定及采购人要求。
1.3.7	政府采购政策落实	**（1）进口产品：本项目不接受进口产品。** （2）落实中小企业、监狱企业、残疾人福利企业政府采购政策。 **1）本项目所属行业：软件和信息技术服务业** 2）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）的要求，以及河南省财政厅政府采购监督管理处发布的“关于进一步加大政府采购支持中小企业力度的通知”对小型、微型企业及监狱企业产品的价格给予10%～20%的扣除，用扣除后的价格参与评审，本项目的扣除比例为：**小型企业扣除10%，微型企业扣除10%，监狱企业10%。** 3）根据《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，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受预留份额、评审中价格扣除等促进中小企业发展的政府采购政策。向残疾人福利性单位采购的金额，计入面向中小企业采购的统计数据。残疾人福利性单位属于小型、微型企业的，不重复享受政策，价格扣除比例同小微企业。 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《政府采购促进中小企业发展管理办法》（财库[2020]46号）规定的中小企业扶持政策。 参加政府采购活动的中小企业应当提供《中小企业声明函》；监狱企业应当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；残疾人福利性单位应当提供《残疾人福利性单位声明函》。 注：依据《政府采购促进中小企业发展管理办法》（财库[2020]46号）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）政府采购节能产品、环境标志产品 1）政府采购节能产品、环境标志产品实施品目清单管理。财政部、发展改革委、生态环境部等部门根据产品节能环保性能、技术水平和市场成熟程度等因素，确定实施政府优先采购和强制采购的产品类别及所依据的相关标准规范，以品目清单的形式发布并适时调整。依据品目清单和认证证书实施政府优先采购和强制采购。 2）采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。关于政府采购节能产品、环境标志产品的相关规定依据《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）。 3）如本项目采购产品属于实施政府强制采购品目清单范围的节能产品，则供应商所报产品必须获得国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，**否则响应无效；** 4）非政府强制采购的节能产品或环境标志产品，依据品目清单和认证证书实施政府优先采购。 （4）正版软件 各级政府部门在购置计算机办公设备时，必须采购预装正版操作系统软件的计算机产品，相关规定依据《国家版权局、信息产业部、财政部、国务院机关事务管理局关于政府部门购置计算机办公设备必须采购已预装正版操作系统软件产品的通知》（国权联〔2006〕1 号）、《国务院办公厅关于进一步做好政府机关使用正版软件工作的通知》（国办发〔2010〕47 号）、《财政部关于进一步做好政府机关使用正版软件工作的通知》（财预〔2010〕536 号）。 （5）网络安全专用产品

		根据国家互联网信息办公室 工业和信息化部 公安部 财政部 国家认证认可监督管理委员会《关于调整网络安全专用产品安全管理有关事项的公告》2023 年第 1 号规定，自 2023 年 7 月 1 日起，列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。自 2023 年 7 月 1 日起，停止颁发《计算机信息系统安全专用产品销售许可证》（简称销售许可证），产品生产者无需申领。此前已经获得销售许可证的产品在有效期内可继续销售或者提供。国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会统一公布和更新符合要求的网络关键设备和网络安全专用产品清单，供社会查询和使用。 （6）采购需求标准 商品包装、快递包装政府采购需求标准（试行） 为助力打好污染防治攻坚战，推广使用绿色包装，根据财政部关于印发《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》的通知（财办库〔2020〕123 号），本项目如涉及商品包装和快递包装的应满足相关要求。 （7）强制性产品认证 所投产品已列入国家强制性产品认证，须提供通过认证的有关证明材料，否则响应无效。 （8）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）要求，采购人或采购代理机构将查询供应商信用记录。 1）信用信息查询渠道：“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（http://www.ccgp.gov.cn）。 2）信用信息查询截止时点：本项目资格审查结束时间。

		3）信用信息查询记录和证据留存的具体方式：信用信息查询记录将以网页打印稿形式与其他采购文件一并保存。 4）信用信息的使用规则：如供应商为“信用中国”网站（www.creditchina.gov.cn）中列入失信被执行人或重大税收违法失信主体的供应商，或为中国政府采购网（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单中被财政部门禁止参加政府采购活动的供应商，**则其响应将被拒绝。**
1.4.1	供应商资格要求	1、满足《中华人民共和国政府采购法》第二十二条规定。 2、落实政府采购政策需满足的资格要求：无。 3、本项目的特定资格要求： 3.1 具有公安部第三研究所颁发的有效的《网络安全等级测评与检测评估机构服务认证证书》。 3.2 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名单、重大税收违法失信主体名单、政府采购严重违法失信行为记录名单的供应商，拒绝参与本项目政府采购活动。[查询渠道：“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）]。 3.3 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。
1.4.2	是否接受联合体投标	本项目不接受联合体投标
1.9.1	实质性要求和条件	**以下内容为竞争性磋商文件的实质性要求和条件，供应商存在下列情况之一的，响应无效：** **（1）未按照采购文件的规定提交投标承诺函的；** **（2）响应文件未按竞争性磋商文件要求签署、盖章的，或无法定代表人签字，或签字人无法定代表人有效授权的；** **（3）不具备竞争性磋商文件中规定的资格要求，资格审查不合格的；** **（4）报价不唯一，出现有选择的报价或替代方案的；**

		（5）报价超过竞争性磋商文件中规定的预算金额或者最高限价的； **（6）磋商有效期不足的；** **（7）服务期限不满足竞争性磋商文件要求的；** **（8）质量要求不满足竞争性磋商文件要求的；** **（9）“响应文件制作机器码一致”的；** **（10）响应文件含有采购人不能接受的附加条件的；** **（11）磋商小组认为供应商的报价明显低于其他通过符合性审查供应商的报价，有可能影响服务质量或者不能诚信履约的，应当要求其在磋商现场合理的时间内提供书面说明，必要时提交相关证明材料；供应商不能证明其报价合理性的，磋商小组应当将其作为无效响应处理；** **（12）法律、法规和竞争性磋商文件规定的其他无效情形。**
3.1	投标语言	供应商提交的响应文件以及供应商与采购方就有关投标的所有来往函电均应使用中文书写。供应商提供的外文资料应附有相应中文译本，并以中文译本为准。
3.2	计量单位	除在竞争性磋商文件的技术规格中另有规定外，计量单位应使用中华人民共和国法定计量单位。
3.4.7	磋商报价	**（1）根据采购文件规定的服务和责任范围，供应商应对投标项目进行总报价。供应商提供的投标报价应包括项目合同项下供应商提供技术、人员、专用设备及工具、检验检测费、技术服务、验收、售后服务、税金等的全部责任和义务。供应商未单独列明的分项价格将视该项目的费用已包含在其他分项中，合同执行中不另行支付。对招标文件中未详细列明的，但为保证项目正常运行所需要的所有费用均计入投标总价中。** **（2）供应商应熟练掌握河南省公共资源交易中心交易系统的操作流程。评审过程中磋商最终报价发起后，系统会自动向供应商发出通知，各供应商须保持在线，及时关注系统提醒，并在规定的时间内完成相关工作，在规定时间内没有提交最后报价**

		的供应商，视同退出(无效)磋商。
3.4.8	最高限价	**（1)本项目最高限价为：人民币叁佰陆拾万元(¥：3600000.00)；** **（2）供应商的投标报价超出最高限价的按无效标处理。**
3.5.1	磋商有效期	90 日
3.6	投标承诺函	供应商应按采购文件要求提供投标承诺函，未提供的视为无效投标。
3.7.2	**资格证明材料**	**参加本项目磋商采购活动的供应商应具备本项目竞争性磋商文件规定的条件，应当提供以下要求的证明材料，未按要求提供或提供不全的视为无效响应。** **（1）具有独立承担民事责任的能力（提供有效的企业法人营业执照副本或法人证书或其他组织、自然人的有效证照）；** **（2）具有公安部第三研究所颁发的有效的《网络安全等级测评与检测评估机构服务认证证书》（提供有效的认证证书）；** **（3）具有良好的商业信誉和健全的财务会计制度（提供完整的2023 年度或2024 年度经审计的财务报告或基本户开户行出具的资信证明）；** **（4）有依法缴纳税收和社会保障资金的良好记录(提供近六个月内任意 1 个月的纳税及社保缴纳证明，如依法免税或纳税零申报须提供相关证明材料）；** **（5）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名单、重大税收违法失信主体名单、政府采购严重违法失信行为记录名单的供应商，拒绝参与本项目政府采购活动。[查询渠道：“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）]；** **（6）具有履行合同所必需的设备和专业技术能力（提供声明）；** **（7）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（提供声明）。** **（8）单位负责人为同一人或者存在直接控股、管理关系的不同**

		供应商，不得参加同一合同项下的政府采购活动。（提供声明）
3.9.3	签字、盖章要求	供应商在制作响应文件时，应将磋商文件格式中明确签字盖章的内容，电子签章或加盖公章（包括企业电子签章或公章、个人电子签章或签名）。
3.9.5	响应文件份数	**加密的电子响应文件壹份（*.hntf 格式，在河南省公共资源交易平台指定位置上传）。**
4.1.1	响应文件加密要求	**加密的电子响应文件（*.hntf 格式）应按河南省公共资源交易平台要求进行加密，在交易平台指定位置上传。供应商未按要求进行加密所产生的所有责任与结果，均由供应商自行承担。**
4.2.1	响应文件递交截止时间	详见磋商公告。
4.2.3	响应文件递交/上传	加密电子响应文件须按规定在河南省公共资源交易中心电子交易平台中加密递交/上传。
5.1.1	磋商文件开启时间和地点	时间：2025 年 8 月 5 日 9：00（北京时间） 地点：河南省公共资源交易中心电子交易平台。
5.2.1	磋商小组	采购人将根据项目的特点依法组建3人及以上单数的磋商小组，其成员由从政府采购专家库中随机抽取的评审专家和采购人代表组成，其中评审专家不得少于成员总数的三分之二。
6.2	成交结果公告 发布媒介	《河南省公共资源交易中心网》、《河南省政府采购网》
6.5.1	履约担保	/
6.6.1	签订合同	采购人和成交供应商应当自成交通知书发出之日起 15 天内，根据竞争性磋商文件和成交供应商的响应文件订立书面合同。
6.8	招标代理服务费	☑收取采购代理服务费： 1.收费对象： □采购人 ☑成交供应商 2.收费标准及金额： 本项目采购代理服务费根据成交金额由中标（成交）人依据《河南省招标代理服务收费指导意见》豫招协【2023】002 号有关规

		定向采购代理机构交纳。 3.代理服务费缴纳方式：以转账、电汇等形式转出（汇款信息需注明：项目编号+代理服务费） 4.代理服务费收款账户信息： 采购代理机构开户名称：河南省国贸招标有限公司 采购代理机构开户行：中信银行郑州南阳路支行 账号：7392410182600025233
7.1	解释权	本竞争性磋商文件的解释权属于采购人和采购代理机构。
7.2	未尽事宜	未尽事宜按国家有关规定执行。
7.3	其他事项	**本项目采用电子招标投标方式，通过河南省公共资源交易中心交易平台进行电子化招标投标，供应商应按交易平台要求办理相应事项。** **本项目竞争性磋商须在线进行磋商报价，各供应商应及时关注河南省公共资源交易中心平台，在规定时间内进行线上报价。如未在规定时间内进行报价，所产生的责任和不利影响由供应商自行承诺。**
8.2.1	接收质疑函的方式	供应商应在法定质疑期内以书面形式提出质疑/异议，并按要求提供质疑函及相关证明材料。
8.2.2	质疑函接收联系事宜	接收单位：河南省国贸招标有限公司 地　址：郑州市农业路 72 号国际企业中心 B 座三楼东侧 联系人：常宗义、刘江 电　话：0371-69136959
	质疑/异议回复方式	采购人或采购代理机构在规定时间内进行质疑/异议的回复。

一、说明

1.1 适用范围

本竞争性磋商文件仅适用于河南省教育考试院信息系统安全服务项目及其伴随服务。

1.2 定义

1.2.1 采购人:“供应商须知前附表”中所述的、依法进行招标采购的国家机关、事业单位、团体组织。

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

1.2.3 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。

1.2.4 成交供应商：接到并接受成交通知，最终被授予合同的供应商。

1.2.5 本竞争性磋商文件的解释权属于采购人和采购代理机构。

1.3 招标项目概况

1.3.1 项目名称：见供应商须知前附表。

1.3.2 项目编号：见供应商须知前附表。

1.3.3 招标范围：见供应商须知前附表。

1.3.4 服务期限：见供应商须知前附表。

1.3.5 合同履行期限：见供应商须知前附表。

1.3.6 质量要求：见供应商须知前附表。

1.3.7 政策落实：见供应商须知前附表。

1.4 供应商资格要求

1.4.1 供应商应具备承担本项目的资格条件、能力和信誉，合格供应商的资格条件：见供应商须知前附表。

1.4.2 联合体投标：见供应商须知前附表。

1.5 合格的服务

无论采购文件中是否要求，供应商所投服务均应符合国家强制性标准，满足采购人需求。

1.6 投标费用

供应商应承担其参与本次投标所涉及的一切费用。不论投标结果如何，采购人或代理机构无义务亦无责任承担这些费用。

1.7 保密

参与招投标活动的各方应对竞争性磋商文件和响应文件中的商业和技术等秘密保密，否

则应承担相应的法律责任。

1.8 投标预备会

本项目不组织投标预备会。

1.9 响应和偏差

1.9.1 响应文件应当对竞争性磋商文件的实质性要求和条件做出满足性或更有利于采购人的响应，否则，供应商的响应将被按无效标处理。实质性要求和条件见供应商须知前附表。

1.9.2 供应商应根据竞争性磋商文件的要求对竞争性磋商文件做出响应。

1.9.3 响应文件对竞争性磋商文件的商务偏差，应在响应文件的商务偏离表中列明，除列明的内容外，视为供应商响应竞争性磋商文件的全部商务要求。

1.10 市场主体信息库

1.10.1 市场主体提交的全部登记信息必须真实准确、完整规范、合法有效。如未及时更新信息或者弄虚作假的，自行承担相应的后果及责任。

1.10.2 市场主体完成信息登记及 CA 数字证书办理后,通过省公共资源交易平台参与交易活动，其行为视为市场主体自愿、真实的交易行为。

1.10.3 市场主体登记的信息将在中心网站相关栏目对外公开，接受社会监督。

1.10.4 供应商编制响应文件时，涉及营业执照、资质、业绩、获奖、人员、财务、社保、纳税、各类证书等内容，必须在市场主体信息库中已登记的信息中选取。供应商应及时对市场主体信息库的相关内容进行补充、更新。

1.10.5 有关市场主体信息库的更多信息，请登录河南省公共资源交易中心网查询。

二、竞争性磋商文件

2.1 竞争性磋商文件构成

2.1.1 竞争性磋商文件由下述部分组成：

（1）竞争性磋商公告

（2）供应商须知

（3）评审方法和标准

（4）合同条款及格式

（5）项目需求

（6）响应文件格式

根据本章第 2.2 款对竞争性磋商文件所作的澄清、修改，构成竞争性磋商文件的组成部

分。

2.1.2 除非有特殊要求，竞争性磋商文件不单独提供招标项目所在地的自然环境、气候条件、公用设施等情况，供应商被视为熟悉上述与履行合同有关的一切情况。

2.1.3 供应商应清楚竞争性磋商文件应该直接从竞争性磋商公告公布的途径获得，根据复制的竞争性磋商文件编制的响应文件将被拒收。

2.2 竞争性磋商文件的澄清或者修改

2.2.1 供应商应仔细阅读和检查竞争性磋商文件的全部内容。如发现缺页或附件不全，应及时向采购人提出，以便补齐。如对竞争性磋商文件有疑问，须在收到竞争性磋商文件之日或者竞争性磋商文件公告期限届满之日起三个工作日内，在交易平台上进行提问，要求采购人对竞争性磋商文件予以澄清。采购人和采购代理机构对潜在供应商在规定期限内提交的疑问将视情况以书面方式予以答复。在规定的时间内未提出疑问的，将被视为完全理解并接受竞争性磋商文件的全部内容。

2.2.2 除非采购人认为确有必要答复，否则，采购人有权拒绝回复供应商在本章第 2.2.1 项规定的时间后的任何澄清要求。

2.2.3 采购人或者采购代理机构可以对已发出的采购文件进行必要的澄清或者修改，但不得改变采购标的和资格条件。澄清或者修改的内容为采购文件的组成部分。澄清或者修改的内容可能影响响应文件编制的，采购人或者采购代理机构在响应截止时间至少 5 日前，通知所有获取采购文件的潜在供应商；不足 5 日的，顺延提交响应文件的截止时间。

2.2.4 磋商文件的澄清或者修改将通过交易平台系统内部“答疑文件”告知供应商，发布给所有获取磋商文件的供应商，并在原公告发布媒体上发布澄清公告，但不指明澄清问题的来源。各供应商须重新下载最新的答疑文件，以此编制响应文件。

2.2.5 因交易中心平台在开标前供应商获取采购文件情况具有保密性，供应商在响应截止时间前须自行查看项目进展、变更通知、澄清及回复，因供应商未及时查看而造成的后果自行承担。

2.3 提交响应文件截止时间的推迟

采购人可以视采购具体情况，推迟提交响应文件截止时间和磋商时间，但至少应当在竞争性磋商文件要求提交响应文件的截止时间三日前，将变更时间通知所有竞争性磋商文件收受人，并在指定的信息发布媒体上发布变更公告。

三、响应文件的编制

3.1 投标语言

供应商提交的响应文件以及供应商与招标方就有关投标的所有来往函电均应使用中文书写。供应商提供的外文资料应附有相应中文译本，并以中文译本为准。

3.2 计量单位

除在竞争性磋商文件的项目需求中另有规定外，计量单位应使用中华人民共和国法定计量单位。

3.3 响应文件的组成

3.3.1 供应商应仔细阅读竞争性磋商文件的所有内容，按竞争性磋商文件的要求编制响应文件；供应商应保证所提供的全部资料的真实性、准确性、有效性，并使其对竞争性磋商文件的实质性要求做出完全的响应，否则，其响应可能被拒绝。

3.3.2 响应文件中应包含但不限于下列内容：

一、封面

二、评审资料

供应商编制响应文件时，涉及营业执照、资质、业绩、获奖、人员、财务、社保、纳税、各类证书等内容，必须在市场主体信息库中已登记的信息中选取。提供的具体内容及要求按磋商文件相应评审因素提供。

供应商利用投标文件制作工具制作响应文件时，评审资料部分是从主体信息库相应菜单中已录入内容进行挑选，之后形成信息表，同时获取对应扫描件进行展示。

三、报价一览表、

四、中小企业声明函（如有）

五、其他内容

1）磋商声明；

2）报价表；

3）法定代表人身份证明或附有法定代表人身份证明的授权委托书；

4）投标承诺函；

5）费用报价及组成分析和说明；

6）中小企业声明函（如有）；

7）监狱企业证明材料（如有）；

8）残疾人福利性单位声明函（如有）；

9）商务条款偏离表；

10）供应商资格审查资料；

11）业绩清单；

12）拟投入人员情况；

13）项目需求偏差表；

14）项目服务方案；

15）供应商认为需要加以说明的其他内容。

3.4 磋商报价

3.4.1 磋商报价应包括国家规定的增值税税金，增值税税金按一般计税方法计算。

3.4.2 除非供应商须知前附表另有规定，供应商提供的所有货物和服务均采用人民币报价。

3.4.3 供应商根据上述规定所作分项报价的目的只是为了评标时对响应文件进行比较的方便，但并不限制采购人订立合同的权力。

3.4.4 除非磋商文件另有规定，只允许有一个最终报价，任何有选择的报价或替代方案将导致响应无效。

3.4.5 供应商应充分了解该项目的总体情况以及影响磋商报价的其他要素，供应商不得以任何理由在开标后对磋商报价予以修改，报价在投标有效期内是固定的，不因任何原因而改变。任何包含价格调整要求和条件的投标，将被视为非实质性响应投标而予以拒绝。

3.4.6 磋商报价为各分项报价金额之和，磋商报价与分项报价的合价不一致的，应以各分项合价累计数为准，修正投标报价；如分项报价中存在缺漏项，则视为缺漏项价格已包含在其他分项报价之中。

3.4.7 磋商报价的其他要求：见供应商须知前附表。

3.4.8 本项目预算金额及最高限价：见供应商须知前附表。

3.5 磋商有效期

3.5.1 除供应商须知前附表另有规定外，磋商有效期为 90 日。

3.5.2 在磋商有效期内，供应商撤销响应文件的，应承担竞争性磋商文件和法律规定的责任。

3.5.3 出现特殊情况需要延长磋商有效期的，采购人以书面形式通知所有供应商延长磋商有效期。供应商应予以书面答复，同意延长的，但不得要求或被允许修改其响应文件；供应商拒绝延长的，其响应失效。

3.6 投标承诺函

供应商应按采购文件要求提供投标承诺函，未提供的视为无效响应。

3.7 供应商资格证明材料

3.7.1 供应商应按竞争性磋商文件的规定提供相应的资格证明材料，作为响应文件的一部分，以证明其有资格进行响应和有能力履行合同。

3.7.2 供应商须提供的资格证明材料：见供应商须知前附表。

3.8 备选投标方案

除供应商须知前附表另有规定外，供应商不得递交备选投标方案。允许供应商递交备选投标方案的，只有成交供应商所递交的备选投标方案方可予以考虑。磋商小组认为成交供应商的备选投标方案优于其按照磋商文件要求编制的投标方案的，采购人可以接受该备选投标方案。

3.9 响应文件的编制

3.9.1 响应文件应按第六章“响应文件格式”进行编写，如有必要，可以增加附页，作为响应文件的组成部分。格式中如供应商响应不涉及的内容，可以不予提供；采购文件未提供格式的响应内容，供应商可自行拟定格式。

3.9.2 响应文件应当对采购文件有关采购内容、服务期限、合同履行期限、质量要求、投标有效期、投标承诺函等实质性内容作出响应。响应文件在满足采购文件实质性要求的基础上，可以提出比采购文件要求更有利于采购人的承诺。

3.9.3 磋商声明及对响应文件的澄清、说明和补正应由供应商的法定代表人（单位负责人）或其授权的代理人签字或盖单位章。由供应商的法定代表人（单位负责人）签字的，应附法定代表人（单位负责人）身份证明，由代理人签字的，应附授权委托书，身份证明或授权委托书应符合第六章“响应文件格式”的要求。响应文件应尽量避免涂改、行间插字或删除。如果出现上述情况，改动之处应由供应商的法定代表人（单位负责人）或其授权的代理人签字或盖单位章。

3.9.4 供应商编制响应文件时，涉及营业执照、资质、业绩、获奖、人员、财务、社保、纳税、各类证书等内容，必须在市场主体信息库中已登记的信息中选取。供应商（供应商）应及时对市场主体信息库的相关内容进行补充、更新。

3.9.5 供应商应按照供应商须知前附表的要求提供响应文件。

（1）加密的电子响应文件壹份（*.hntf 格式，在交易平台指定位置上传）；

3.9.6 采购人不接收以电报、电话、传真、邮件形式的投标。

四、响应文件的递交

4.1 响应文件的密封和标记

4.1.1 供应商应当按照采购文件和电子招标投标交易平台的要求加密响应文件，具体要求见供应商须知前附表。

4.2 响应文件的递交

4.2.1 加密电子响应文件上传截止时间：见供应商须知前附表。

4.2.2 供应商应在投标截止时间前通过河南省公共资源交易平台上传加密的电子响应文件（*.hntf）到交易平台的指定位置，并确认上传成功。请供应商在上传时认真检查上传响应文件是否完整、正确。供应商因交易平台投标系统问题无法上传电子响应文件时，请在工作时间与交易平台联系。

4.2.3 加密电子响应文件须须在投标截止时间前通过“河南省公共资源交易中心（https://hnsggzyjy.henan.gov.cn//）”电子交易平台中递交/上传，加密电子响应文件逾期或未按规定递交/上传的，采购人不予受理。

4.3 响应文件的修改和撤回

4.3.1 在本章 4.2.1 项规定的投标截止时间前，供应商可以对所上传的响应文件进行补充、修改或者撤回，并书面通知采购人或者采购代理机构。补充、修改的内容应当按照采购文件要求签署、盖章后，作为响应文件的组成部分。

4.3.2 供应商在投标截止时间前可以撤回已提交的响应文件的。

4.3.3 从投标截止时间至供应商在响应文件中载明的投标有效期满期间，供应商不得撤销其响应。

五、磋商与评审

5.1 磋商时间和地点

5.1.1 采购人和采购代理机构将在“供应商须知前附表”中规定的时间和地点组织磋商会议。供应商无需到交易中心现场参加磋商会议，磋商会议采用“远程不见面”方式，开标大厅的网址 https://hnsggzyjy.henan.gov.cn/BidOpening/bidopeninghallaction/hall/login。所有供应商须在磋商文件规定的响应文件提交截止时间前，登录远程开标大厅，在线准时参加磋商会议活动，并在规定的时间内对响应文件进行解密、答疑澄清（如需要）、最后报价等。

5.1.2 供应商须在供应商须知前附表规定的时间内完成响应文件的解密。由于供应商的自身原因，在规定时间内解密不成功的，其响应文件将被拒绝。

5.1.3 供应商在“河南省公共资源交易中心（http://hnsggzyjy.henan.gov.cn/）”网站下载采购文件成功后，如未在磋商文件规定的“响应文件提交截止时间”前成功上传或误传加密的响应文件，而导致的解密失败，其响应文件将被拒绝。

5.1.4 供应商代表对磋商会议有疑义的，应当在磋商过程中通过交易系统提出。

5.1.5 在供应商须知前附表规定的时间内完成响应文件解密的供应商不足 3 家的，将不再进行磋商（特殊情况除外）。

5.2 评审

5.2.1 磋商小组

（1）采购人将根据采购项目的特点依法组建 3 人及以上单数的磋商小组，除国务院财政部门规定的情形外，其成员由从政府采购专家库中随机抽取的评审专家和采购人代表组成，其中评审专家不得少于成员总数的三分之二。

（2）评审专家与参加采购活动的供应商存在下列利害关系之一的,应当回避:

1）参加采购活动前三年内,与供应商存在劳动关系,或者担任过供应商的董事、监事,或者是供应商的控股股东或实际控制人；

2）与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

3）与供应商有其他可能影响招标采购活动公平、公正进行的关系。

评审专家发现本人与参加采购活动的供应商有利害关系的,应当主动提出回避。采购人或者采购代理机构发现评审专家与参加采购活动的供应商有利害关系的,应当要求其回避。

（3）评审中因磋商小组成员缺席、回避或者健康等特殊原因导致磋商小组组成不符合规定的，采购人或者采购代理机构应当依法补足后继续评审。被更换的磋商小组成员所作出的评审意见无效。无法及时补足磋商小组成员的，采购人或者采购代理机构应当停止评审活动，封存所有响应文件和磋商、评审资料，依法重新组建磋商小组进行评审。原磋商小组所作出的评审意见无效。

5.2.2 评审过程

（1）磋商小组负责具体评审事务，对供应商的响应文件进行资格审查、符合性审查，以确定其是否满足供应商资格要求、竞争性磋商文件的实质性要求；对通过资格审查、符合性审查的供应商，磋商小组将与供应商进行磋商。

（2）磋商小组在对响应文件的有效性、完整性和响应程度进行审查时，可以要求供应商对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容等作出必要的澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。

（3）磋商小组要求供应商澄清、说明或者更正响应文件应当以交易中心系统内发出的澄清函为准。供应商的澄清、说明或者更正应当由法定代表人或其委托代理人签字或者加盖单

位电子公章。磋商小组不接受供应商主动提出的澄清、说明。

（4）对于响应文件中不构成实质性偏差的不正规、不一致或不规则，磋商小组可以接受，但这种接受不能损害或影响任何供应商的相对排序。

（5）磋商结束后，磋商小组应当要求所有实质性响应的供应商在规定时间内提交最后报价，提交最后报价的供应商不得少于 3 家。

（6）已提交响应文件的供应商，在提交最后报价之前，可以根据磋商情况退出磋商。

（7）供应商应熟练掌握河南省公共资源交易中心交易系统的操作流程。评审过程中磋商最终报价发起后，系统会自动向供应商发出通知，各供应商须保持在线，及时关注系统提醒，并在规定的时间内完成相关工作，在规定时间内没有提交最后报价的供应商，视同退出(无效)磋商。

（8）经磋商确定最终采购需求和提交最后报价的供应商后，由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。

（9）评审时，磋商小组各成员应当独立对每个有效响应的文件进行评价、打分，然后汇总每个供应商每项评分因素的得分。磋商文件中没有规定的评审标准不得作为评审依据。

（10）磋商小组将根据综合评分情况，按照评审得分由高到低顺序推荐 3 名成交候选供应商，并编写评审报告。评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的，按照技术指标得分高低推荐。

5.2.3 评审原则

评审活动遵循公平、公正、科学和择优的原则。

5.2.4 评审方法

本此磋商采用综合评分法，具体内容详见竞争性磋商文件第三章评审方法和标准。

5.2.5 废标条件

出现下列情形之一，将导致项目废标即本项目的所有投标被拒绝：

（1）提交最后报价的供应商不足三家；

（2）出现影响采购公正的违法、违规行为的；

（3）供应商的报价均超过了采购预算或最高限价，采购人不能支付的；

（4）因重大变故，采购任务取消的。

5.2.6 保密原则

（1）评审将在严格保密的情况下进行。

（2）除了依法向监管部门提供情况外，磋商小组成员及与评审活动有关的工作人员不得

泄露有关响应文件的评审和比较、成交候选供应商的推荐以及与评审有关的其他情况。

（3）供应商试图影响招标采购单位和磋商小组的任何活动，将导致其响应被拒绝，并承担相应的法律责任。

六、中标和合同

6.1 确定成交供应商

采购代理机构应当在评审结束后 2 个工作日内将评审报告送采购人。采购人应当自收到评审报告之日起 5 个工作日内，在评审报告确定的成交候选供应商名单中按顺序确定成交供应商。采购人在收到评审报告 5 个工作日内未按评审报告推荐的成交候选供应商顺序确定成交供应商，又不能说明合法理由的，视同按评审报告推荐的顺序确定排名第一的成交候选供应商为成交供应商。

6.2 成交结果公告

采购人或者采购代理机构应自成交供应商确定之日起 2 个工作日内，将在供应商须知前附表规定的媒体上公告成交结果，供应商可通过相关发布媒体查询成交结果。成交结果公告期限为 1 个工作日。

供应商对成交结果有异议的，须在成交结果公告发布之日起 7 个工作日内对成交结果以书面形式提出质疑，质疑应当有明确的请求和必要的证明材料，供应商需对质疑内容的真实性承担责任，逾期提出的质疑，采购人或采购代理机构将不予以受理。

6.3 接受和拒绝任何或所有投标的权利

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

6.4 成交通知书

6.4.1 在公告成交结果的同时，采购人或者采购代理机构将向成交供应商发出成交通知书。

6.4.2 成交通知书发出后，采购人不得违法改变成交结果，成交供应商无正当理由不得放弃成交。

6.4.3 成交通知书是合同的组成部分。

6.5 履约担保

6.5.1 在签订合同前，成交供应商应按供应商须知前附表的规定和竞争性磋商文件第四

章“合同条款及格式”的规定向采购人提交履约担保。

6.5.2 成交供应商不能按本章第 6.5.1 项要求提交履约担保的，视为放弃中标。

6.6 签订合同

6.6.1 采购人和成交供应商应当自成交通知书发出之日起 15 天内，根据竞争性磋商文件和成交供应商的响应文件订立书面合同。所签订的合同不得对竞争性磋商文件确定的事项和成交供应商响应文件作实质性修改。

采购人不得向成交供应商提出任何不合理的要求作为签订合同的条件。

6.6.2 竞争性磋商文件、成交供应商的响应文件及其澄清文件等，均为签订合同的依据。

6.6.3 成交通知书发出后，成交供应商放弃成交（不可抗力因素除外），须承担相应的法律责任。

6.6.4 成交供应商拒绝与采购人签订合同的，采购人可以按照评审报告推荐的成交候选供应商名单排序，确定下一候选人为成交供应商，也可以重新开展招标采购活动。

6.7 纪律和监督

6.7.1 对采购人的纪律要求

采购人不得泄露招标投标活动中应当保密的情况和资料，不得与供应商串通损害国家利益、社会公共利益或者他人合法权益。

6.7.2 对供应商的纪律要求

供应商不得相互串通投标或者与采购人串通投标，不得向采购人或者磋商小组成员行贿谋取中标，不得以他人名义投标或者以其他方式弄虚作假骗取中标；供应商不得以任何方式干扰、影响评审工作。

6.7.3 对磋商小组成员的纪律要求

磋商小组成员不得收受他人的财物或者其他好处，不得向他人透露对响应文件的评审和比较、成交候选供应商的推荐情况以及评审有关的其他情况。在评审活动中，磋商小组成员应当客观、公正地履行职责，遵守职业道德，不得擅离职守，影响评审程序正常进行，不得使用第三章“评审办法和标准”没有规定的评审因素和标准进行评审。

6.7.4 对与评审活动有关的工作人员的纪律要求

与评审活动有关的工作人员不得收受他人的财物或者其他好处，不得向他人透露对响应文件的评审和比较、成交候选供应商的推荐情况以及评审有关的其他情况。在评审活动中，与评审活动有关的工作人员不得擅离职守，影响评审程序正常进行。

6.8 招标代理服务费

详见供应商须知前附表

七、需要补充的其他内容

需要补充的其他内容：见供应商须知前附表。

八、质疑和投诉

8.1 政府采购供应商提出质疑和投诉应当坚持依法依规、诚实信用原则。

8.2 质疑函的接收

8.2.1 接收质疑函的方式：详见供应商须知前附表。

8.2.2 质疑函接收联系事宜：详见供应商须知前附表。

8.2.3 质疑/异议回复方式：详见供应商须知前附表。

8.3 供应商可以委托代理人进行质疑和投诉。其授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人签字或者盖章，并加盖公章。代理人提出质疑和投诉，应当提交供应商签署的授权委托书。。

8.4 以联合体形式参加政府采购活动的，其质疑和投诉应当由组成联合体的所有供应商共同提出。

8.5 供应商认为采购文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起 7 个工作日内，以书面形式向采购人、采购代理机构提出质疑；供应商应在法定质疑期内一次性提出针对同一采购程序环节的质疑。。

8.6 提出质疑的供应商应当是参与所质疑项目采购活动的供应商。潜在供应商已依法获取其可质疑的采购文件的，可以对该文件提出质疑。对采购文件提出质疑的，应当在获取采购文件或者采购文件公告期限届满之日起 7 个工作日内提出。

8.7 供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

（一）供应商的姓名或者名称、地址、邮编、联系人及联系电话；

（二）质疑项目的名称、编号；

（三）具体、明确的质疑事项和与质疑事项相关的请求；

（四）事实依据；

（五）必要的法律依据；

（六）提出质疑的日期。

供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

质疑函格式详见附件 1。

8.8 采购人、采购代理机构不得拒收质疑供应商在法定质疑期内发出的质疑函，应当在收到质疑函后 7 个工作日内作出答复，并以书面形式通知质疑供应商和其他有关供应商。

8.9 质疑供应商对采购人、采购代理机构的答复不满意，或者采购人、采购代理机构未在规定时间内作出答复的，可以在答复期满后 15 个工作日内按《政府采购质疑和投诉办法》（财政部令第 94 号）的规定向财政部门提起投诉。

8.10 投诉人在全国范围 12 个月内三次以上投诉查无实据的，由财政部门列入不良行为记录名单，投诉人有下列行为之一的，属于虚假、恶意投诉，由财政部门列入不良行为记录名单，禁止其 1 至 3 年内参加政府采购活动：

（一）捏造事实;

（二）提供虚假材料;

（三）以非法手段取得证明材料。证据来源的合法性存在明显疑问，投诉人无法证明其取得方式合法的，视为以非法手段取得证明材料。

附件 1：质疑函范本

质疑函范本

一、质疑供应商基本信息

质疑供应商：.....

地址：..... 邮编：.....

联系人：..... 联系电话：.....

授权代表：.....

联系电话：.....

地址：..... 邮编：.....

二、质疑项目基本情况

质疑项目的名称：.....

质疑项目的编号：..... 包号：.....

采购人名称：.....

采购文件获取日期：.....

三、质疑事项具体内容

质疑事项 1：.....

事实依据：.....

.....

法律依据：.....

.....

质疑事项 2

……

四、与质疑事项相关的质疑请求

请求：.....

签字(签章)： 公章：

日期：

质疑函制作说明：

1.供应商提出质疑时，应提交质疑函和必要的证明材料。

2.质疑供应商若委托代理人进行质疑的，质疑函应按要求列明“授权代表”的有关内容，并在附件中提交由质疑供应商签署的授权委托书。授权委托书应载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。

3.质疑供应商若对项目的某一分包进行质疑，质疑函中应列明具体分包号。

4.质疑函的质疑事项应具体、明确，并有必要的事实依据和法律依据。

5.质疑函的质疑请求应与质疑事项相关。

6.质疑供应商为自然人的，质疑函应由本人签字；质疑供应商为法人或者其他组织的，质疑函应由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

第三章 评审方法和标准

一、评审依据

根据有关法律、行政法规，结合本次招标项目实际情况，遵循公平、公正、科学、择优的基本原则，制定本评审办法。

二、磋商小组

2.1 采购人将根据招标采购项目的特点依法组建 3 人及以上单数的磋商小组，除国务院财政部门规定的情形外，其成员由从政府采购专家库中随机抽取的评审专家和采购人代表组成，其中评审专家不得少于成员总数的三分之二。

2.2 评审专家与参加采购活动的供应商存在下列利害关系之一的，应当回避：

1）参加采购活动前三年内，与供应商存在劳动关系，或者担任过供应商的董事、监事，或者是供应商的控股股东或实际控制人；

2）与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

3）与供应商有其他可能影响招标采购活动公平、公正进行的关系。

评审专家发现本人与参加采购活动的供应商有利害关系的，应当主动提出回避。采购人或者采购代理机构发现评审专家与参加采购活动的供应商有利害关系的，应当要求其回避。

2.3 评审中因磋商小组成员缺席、回避或者健康等特殊原因导致磋商小组组成不符合本办法规定的，采购人或者采购代理机构应当依法补足后继续评审。被更换的磋商小组成员所作出的评审意见无效。无法及时补足磋商小组成员的，采购人或者采购代理机构应当停止评审活动，封存所有响应文件和开标、评审资料，依法重新组建磋商小组进行评审。原磋商小组所作出的评审意见无效。

三、评审方法及标准

3.1 本次磋商采用综合评分法。经磋商确定最终采购需求和提交最后报价的供应商后，由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。磋商小组将根据综合评分情况，按照评审得分由高到低顺序推荐 3 名成交候选供应商，并编写评审报告。评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的，按照技术标得分高低推荐。

3.2 采购人或者采购代理机构负责组织评审工作，并履行相关职责；磋商小组负责具体评

审事务，并独立履行相关职责。

3.3 评审步骤

评审分为初步评审、磋商、详细评审三个阶段。

3.4 初步评审

磋商小组对供应商的响应文件进行资格审查、符合性审查，以确定其是否满足供应商资格要求、竞争性磋商文件的实质性要求。

3.4.1 符合性检查依据竞争性磋商文件的规定，从响应文件的有效性、完整性和对竞争性磋商文件的响应程度进行审查，以确定是否对竞争性磋商文件的实质性要求做出响应。

（1）磋商小组将审查响应文件是否完整、总体编制是否有序、文件签署是否合格、供应商是否提交了投标承诺函、有无计算上的错误等。

（2）响应文件报价出现前后不一致的，按照下列规定修正：

1）响应文件中报价一览表（报价表）内容与响应文件中相应内容不一致的，以报价一览表（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，以报价一览表的总价为准，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。修正后的报价经供应商确认后产生约束力，供应商不确认的，其投标无效。

磋商小组认为供应商的报价明显低于其他通过符合性审查供应商的报价，有可能影响工程质量或者不能诚信履约的，应当要求其在评审现场合理的时间内提供书面说明，必要时提交相关证明材料；供应商不能证明其报价合理性的，磋商小组应当将其作为无效投标处理。

3.4.2 实质上响应的磋商应该是与竞争性磋商文件要求的全部条款、条件相符，没有重大偏离。对关键条款的偏离、保留和反对，将被认为是实质上的偏离，属于无效投标被拒绝。磋商小组决定投标的响应性只根据响应文件本身的内容，而不寻求外部的证据。

3.4.3 实质上没有响应竞争性磋商文件要求的投标将被作为无效投标被拒绝。供应商不得通过修正或撤销不符合要求的偏离或保留从而使其投标成为实质上响应的投标。**如发现下列情况之一的，其投标将被作为无效投标被拒绝：**

（1）未按照采购文件的规定提交投标承诺函的；

（2）响应文件未按竞争性磋商文件要求签署、盖章的，或无法定代表人签字，或签字人无法定代表人有效授权的；

（3）不具备竞争性磋商文件中规定的资格要求，资格审查不合格的；

（4）报价不唯一，出现有选择的报价或替代方案的；

（5）报价超过竞争性磋商文件中规定的预算金额或者最高限价的；

（6）磋商有效期不足的；

（7）服务期限不满足竞争性磋商文件要求的；

（8）质量要求不满足竞争性磋商文件要求的；

（9）“响应文件制作机器码一致”的；

（10）响应文件含有采购人不能接受的附加条件的；

（11）磋商小组认为供应商的报价明显低于其他通过符合性审查供应商的报价，有可能影响服务质量或者不能诚信履约的，应当要求其在磋商现场合理的时间内提供书面说明，必要时提交相关证明材料；供应商不能证明其报价合理性的，磋商小组应当将其作为无效响应处理；

（12）法律、法规和竞争性磋商文件规定的其他无效情形。

3.4.4 磋商小组只对在通过初步评审，确定为实质性响应的供应商进行下一步磋商。

3.5 磋商

3.5.1 磋商小组对通过初步评审的供应商，磋商小组将与供应商进行磋商。

3.5.2 磋商小组在对响应文件的有效性、完整性和响应程度进行审查时，可以要求供应商对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容等作出必要的澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。

3.5.3 磋商小组要求供应商澄清、说明或者更正响应文件应当以书面形式作出。供应商的澄清、说明或者更正应当由法定代表人或其委托代理人签字或者加盖公章。由委托代理人签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。磋商小组不接受供应商主动提出的澄清、说明。

3.5.4 对于响应文件中不构成实质性偏差的不正规、不一致或不规则，磋商小组可以接受，但这种接受不能损害或影响任何供应商的相对排序。

3.5.5 在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应当及时以书面形

式同时通知所有参加磋商的供应商。

供应商应当按照磋商文件的变动情况和磋商小组的要求重新提交响应文件，并由其法定代表人或授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

3.5.6 磋商结束后，磋商小组应当要求所有实质性响应的供应商在规定时间内提交最后报价，提交最后报价的供应商不得少于 3 家。

3.5.7 供应商应熟练掌握河南省公共资源交易中心交易系统的操作流程。评审过程中磋商最终报价发起后，系统会自动向供应商发出通知，各供应商须保持在线，及时关注系统提醒，并在规定的时间内完成相关工作，在规定时间内没有提交最后报价的供应商，视同退出(无效)磋商。

3.6 详细评审

3.6.1 经磋商确定最终采购需求和提交最后报价的供应商后，由磋商小组按照竞争性磋商文件中规定的评审方法和标准，对提交最后报价的供应商的响应文件和最后报价进行综合评分。

3.6.2 评审时，磋商小组各成员应当独立对每个有效响应的文件进行评价、打分，然后汇总每个供应商每项评分因素的得分。磋商文件中没有规定的评审标准不得作为评审依据。

3.6.3 磋商小组将根据综合评分情况，按照评审得分由高到低顺序推荐 3 名成交候选供应商。评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的，按照技术标得分高低推荐。

3.6.4 评审结束后，磋商小组根据全体评审成员签字的原始评审记录和评审结果编写评审报告。

3.6.5 磋商小组成员对需要共同认定的事项存在争议的，应当按照少数服从多数的原则作出结论。持不同意见的磋商小组成员应当在评审报告上签署不同意见及理由，否则视为同意评审报告。

3.6.6 除资格性检查认定错误、分值汇总计算错误、分项评分超出评分标准范围、客观分评分不一致、经磋商小组一致认定评分畸高、畸低的情形外，采购人或者采购代理机构不得以任何理由组织重新评审。采购人、采购代理机构发现磋商小组未按照磋商文件规定的评审标准进行评审的，应当重新开展采购活动，并同时书面报告本级财政部门。

四、评审因素及评分标准

评分内容		分值	评标标准
价格部分（10 分）		10	（1）落实政府采购政策，对小型、微型企业、监狱企业及残疾人福利性单位产品或服务（以响应文件提供的符合规定的有关证明材料为准）价格给予 10%的扣除，以扣除后的价格计算评标基准价和投标报价。 （2）价格分采用低价优先法计算，即满足采购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 10 分。其他供应商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。
商务部分（15 分）	业绩	5	供应商 2022 年 7 月 1 日以来具有同类的安全技术服务合同： （1）每提供等保测评合同一份得 1 分，最多得 2 分； （2）每提供信息安全服务类合同一份得 1 分，最多得 3 分。 响应文件中须提供合同扫描件，合同不重复计算，未按要求提供不得分。
	认证	5	（1）供应商具有有效的 ISO/IEC27001 信息安全管理体系认证证书，并提供证书扫描件得 2 分，否则不得分。 （2）供应商具有中国网络安全审查认证和市场监管大数据中心（或原中国网络安全审查技术与认证中心）颁发的有效的信息系统安全运维、信息安全风险评估、信息安全应急处理资质证书的得 3 分，否则不得分。
	履职尽责措施	5	具有可行、有效的书面保证技术措施落实关键岗位人员到位的履职承诺和落实不到位的处理承诺。 （1）根据供应商的承诺及相关措施进行横向比较，具有可行、有效的关键岗位人员到位的履职承诺和落实不到位的处理措施等的得 5 分； （2）具有书面保证技术措施落实关键岗位人员到位的履职承诺和落实不到位的处理措施等的得 3 分； （3）履职承诺齐全和落实不到位的处理措施较一般或和落实不到

			位的处理措施有缺项的得 1 分； （4）没有提供具体内容的得 0 分。
技术部分（75 分）	项目需求响应性情况	20	供应商全部满足和响应采购文件的项目需求，得满分 20 分。 加★项是项目重要要求，不可负偏离,若有负偏离按无效投标处理。 非★项每有一项不满足或低于采购文件要求扣 0.5 分，扣完为止。本项得分为零时作无效投标处理。
	需求理解	4	项目的定位和识别准确，总体方案思路清晰、符合实际，具有可操作性；针对本项目特点、难点的分析合理、方案科学，根据投标人需求理解进行综合评审。 （1）理解全面、分析透彻，得 4 分； （2）理解较全面但有不足之处得 2 分； （3）理解一般得 1 分； （4）未提供不得分。
	总体服务方案	6	项目整体服务方案完善，能结合同类项目的服务经验，提出完善的项目实施方案与服务，实施计划操作性强、计划清晰、人员配备合理，根据供应商的方案进行综合评审。 （1）项目实施方案科学、合理、实施计划操作性强、技术手段先进、技术方案完整、人员配备合理的得 6 分； （2）项目实施方案较合理、实施计划操作性较强、技术手段较先进、技术方案较完整、人员配备较合理的得 4 分； （3）项目实施方案一般、实施计划操作性一般、技术手段一般、技术方案一般、人员配备一般、项目实施方案有缺项的得 2 分； （4）未提供不得分。
	等级保护测评服务方案	10	依据各供应商针对本项目等级保护测评实施方案中所包含的流程步骤、测评方法、测评工具、保密措施、项目管理制度、风险方法措施等内容的详细具体程度、科学性和先进性，各项管理制度的规范性，以及评测服务的保密措施、风险防范措施的有效性和可操作性进行综合评审。 （1）项目测评服务方案科学、合理、可操作性强的，得 10 分；

			（2）项目测评服务方案较科学、较合理、具有可操作性的，得 7 分； （3）项目测评服务方案科学性一般、合理性一般、可操作性一般、有缺项的，得 4 分； （4）未提供不得分。
	重点业务保障安全服务方案	10	根据供应商提供的重点业务保障安全服务方案，在现场安全保障、互联网暴露面安全监测与分析服务、内网安全态势监控与分析服务、源代码审计服务、渗透测试服务、漏洞扫描服务、安全加固与补丁服务、专项安全治理服务、网络和数据安全行业监管平台服务、定制开发服务、应急响应服务、应急演练服务、网络安全攻防演习服务、DCMM 数据管理能力成熟度评估服务、安全培训服务等方面方案设计完整性、合理性、可操作性与河南省教育考试院业务系统实际情况契合度等方面进行综合评审。 （1）重点业务保障安全服务方案科学、合理、可操作性强的，得 10 分； （2）重点业务保障安全服务方案较科学、较合理、具有可操作性的，得 7 分； （3）重点业务保障安全服务方案科学性一般、合理性一般、可操作性一般、有缺项的，得 4 分； （4）未提供不得分。
	日常办公网络安全运维服务	4	根据供应商提供的日常办公网络安全运维服务方案，在日常巡检、安全运维、升级及维护等方面方案设计完整性、合理性、可操作性与河南省教育考试院业务系统实际情况契合度等方面进行评审。 （1）日常办公网络安全运维服务方案科学、合理、可操作性强的，得 4 分； （2）日常办公网络安全运维服务较科学、较合理、具有可操作性的，得 2 分； （3）日常办公网络安全运维服务方案科学性一般、合理性一般、

			可操作性一般、有缺项的，得 1 分； （4）未提供不得分。
	安全培训	3	根据供应商的安全培训方案进行评估，要求培训具有针对性和时效性，合理安排培训师资水平、培训课程设置、培训讲义内容、提供本地化的培训设施等进行评审。 （1）安全培训方案科学、合理、可操作性强的，得 3 分； （2）安全培训方案较科学、较合理、具有可操作性的，得 1 分； （3）安全培训方案科学性一般、合理性一般、可操作性一般、安全培训方案有缺项的，得 0.5 分； （4）未提供不得分。
	项目团队	14	根据各供应商拟派项目团队成员情况评分，项目团队成员须为本单位在职人员，拟任人员岗位不得重复使用，人员需提供证书和本单位为其缴纳的社保证明，未按要求提供不得分。 （1）执行项目经理：1 人，需在项目周期内驻场服务。同时具有网络安全等级保护测评师证书(高级)、注册信息安全工程师（CISE）证书，得 4 分。 （2）重点安全保障现场服务人员：所有招生考试业务要求现场派驻人员不低于 5 人。 1）重点安全保障组负责人具有注册信息安全工程师（CISE）和信息安全保障人员认证证书（CISAW 安全运维和 CISAW 风险管理），得 2 分。 2) 除重点安全保障组负责人外，重点安全保障组成员中持有信息安全保障人员认证证书（CISAW 应急服务）、信息安全保障人员认证证书（CISAW 风险管理）、注册信息安全工程师（CISE）证书、软件测评工程师证书，各证书持有人数不少于 1 人，得 2 分。 （3）日常办公安全运维服务人员要求：现场派驻人员不低于 4 人，且均需熟悉招标方业务流程。 1）日常办公安全运维组负责人具有注册信息安全工程师（CISE）和信息安全保障人员认证证书（CISAW 安全运维和 CISAW 风险管

			理)，得 2 分。 2）除日常办公安全运维组负责人外，项目成员中至少 2 人具备渗透测试能力，并持有注册渗透测试工程师（CISP-PTE）证书，得 1 分。 （4）等级保护测评服务人员：项目参与人员不低于 5 人。项目成员中具有网络安全等级保护测评师证书（高级）或信息安全等级测评师证书（高级）的人员不少于 3 人，其中至少 1 名高级测评师需具有高级工程师证书。项目成员中具有网络安全等级测评师证书（中级及以上）或信息安全等级测评师证书（中级及以上）证书人员不少于 2 人，得 3 分。 备注： ①网络/信息安全等级测评师证书的发证机构为中关村信息安全测评联盟或者公安部信息安全等级保护评估中心。 ②注册信息安全工程师（CISE）证书、注册渗透测试工程师（CISP-PTE）证书的发证机构为中国信息安全测评中心。 ③信息安全保障人员认证证书（CISAW）的发证机构为中国网络安全审查认证和市场监管大数据中心（或原中国网络安全审查技术与认证中心）。 ④软件测评工程师证书的发证机构为工业和信息化部教育与考试中心。
	保密管理	2	针对本项目的保密管理方案，包括：保密管理制度、保密保障措施等进行评审。 （1）保密管理方案科学、合理、可操作性强的，得 2 分； （2）保密管理方案较科学、较合理、具有可操作性的，得 1 分； （3）保密管理方案科学性一般、合理性一般、可操作性一般、保密管理方案有缺项的，得 0.5 分； （4）未提供不得分。
	验收方案	2	重点考核验收流程及标准，技术成果移交、档案归档等。包括但不限于：规范性文本、技术成果移交档案、测评报告等样本方案

			进行评审。 （1）验收方案科学、合理、可操作性强的，得 2 分； （2）验收方案较科学、较合理、具有可操作性的，得 1 分； （3）验收方案科学性一般、合理性一般、可操作性一般、验收方案有缺项的，得 0.5 分； （4）未提供不得分。
总计		100 分	

注：

1.全体磋商小组成员对供应商评分的算术平均值即为该供应商最终评审得分。

2.评分和计算结果均保留小数点后 2 位（采用四舍五入法）。

3.磋商小组按各供应商最终评审得分从高到低的顺序向采购人推荐 3 名成交候选供应商。

第四章 合同条款及格式

合同编号：

河南省教育考试院
信息系统安全服务项目合同

甲　　方：

乙　　方：

年　　月

目录

甲方：

乙方：

本合同于_____年____月___日由甲方和乙方按下述条款签署。

在甲方为获得_____（项目名称）_____，经河南省财政厅政府采购处批准，进行了磋商采购。经磋商小组评审并经需方确认，确认乙方以三年服务费总金额：（¥_____元）（以下简称“合同价”）、其中每年度服务费金额为：_____（¥_____元）成交，成为甲方供应商。双方以上述事实为基础，依照《中华人民共和国民法典》、《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》（中华人民共和国国务院令 第 147 号）及其他有关法律、行政法规，遵循平等、自愿、公平和诚实信用的原则，就本服务项目事项协商一致，订立本合同。

第一章 定义

1.1 本合同包含正文《河南省教育考试院信息系统安全服务项目合同书》和附件《项目保密协议书》、《项目采购文件》、《项目响应文件》和其他相关采购文件组成。

1.2 合同双方可根据本次信息系统安全服务项目具体情况，就本合同的未尽事宜协商订立附加条款，作为本合同正式内容的一部分。

1.3 本合同及附件共_____页。

第二章 双方责任与义务

2.1 乙方职责与承诺

2.1.1 乙方依据《信息安全等级保护管理办法》(公通字[2007]43 号)、《信息安全技术 网络安全等级保护基本要求》、《信息安全技术 网络安全等级保护实施指南》、《信息安全等级保护安全建设整改指南》《安全风险评估指南》《安全加固指南》及《安全运维指南》等一系列信息安全标准对甲方的：河南省招生考试考生服务平台、河南省招生考试网上录取系统、河南省招生考试信息网络管理系统、门户网站 实施信息安全等级保护测评服务，评估甲方信息系统安全保护现状及存在的安全风险，并提交《信息系统网络安全等级保护测评报告》，该报告需包含但不限于甲方信息系统的全量资产清单、漏洞修复方案及复测验收标准等，且对甲方系统安全建设提出意见和建议。另外，需负责甲方全院所有网络设备、安全设备、服务器及终端的日常安全巡检、定期漏洞扫描，各项招生考试业务信息系统上线前的源代码安全检测，各项招生考试业务信息系统的定期漏洞扫描、风险评估、渗透测试及安全加固，日常办公运维、内网安全态势监测与分析、互联网暴露面安全监测与分析、重点业务安全保障、专项安全治理、网络攻防演习、安全管理人员的专业技能培训和全院办公人员的安全技术及意识培训等，囊括采购方动态的、整体的安全管理和保障体系的建立。

2.1.2 乙方作为网络安全等级保护测评机构，具体测评资质如下：

1)乙方具有公安部第三研究所颁发的有效的《网络安全等级测评与检测评估机构服务认证证书》。

2.1.3 乙方作为网络安全等级保护测评机构，承诺满足《网络安全等级保护测评机构管理办法》第五条、第十八条、第二十四条、第二十八条中对从事网络安全等级保护测评的机构应当履行义务的要求，具体如下：

1) 应按照国家有关网络安全法律法规规定和标准规范要求，为用户提供科学、安全、客观、公正的等级测评服务。

2) 应采取管理和技术措施保护测评活动中相关数据和信息的安全，不得泄露在测评服务中知悉的商业秘密、重要敏感信息和个人信息；未经等保办同意，不得擅自发布、披露在测评服务中收集掌握的网络信息、系统漏洞、恶意代码、网络攻击等信息。

3) 应加强对测评人员的监督管理，定期组织开展安全保密教育和测评业务培训，签订安全保密责任书，规定其应当履行的安全保密义务和承担的法律责任，并负责检查落实。

4) 测评机构应当建立网络安全应急处置机制和纠纷处理机制，防范测评风险，妥善处理纠纷。

2.1.4 乙方承诺项目实施人员均须具备国家认可的信息安全服务相关职业资质(如网络安全等级保护测评师证书等），所有实施人员名单及证书应于项目启动前报甲方审核备案。乙方应严格遵循《中华人民共和国网络安全法》、GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》（如有新版本则自动适用新版本）、GA/T 1357-2017 等现行有效且适用的国家标准及行业标准，确保服务过程及成果文件全部达到上述标准最新要求。

2.1.5 乙方将为甲方专门成立项目组，指定一位合格的、有足够信息安全服务经验的项目经理，负责甲方和乙方之间的正式交流，领导和推进项目组的全面工作。项目组成员名单、资质、经验需提前报甲方审核。乙方更换项目经理及核心技术人员需提前 30 日书面申请并经甲方书面同意，甲方有权要求更换不合格人员，否则视为乙方违约。乙方应保证项目组人员稳定，未经甲方同意不得随意更换，从而维护服务质量和项目连续性。

2.1.6 乙方的信息安全服务行为受测评主管机关的监督和监管，乙方的主管机关可组织河南省信息安全领域内知名专家、学者参与本项目的评审以及监督。

2.1.7 乙方对甲方所有数据、资料、信息负有长期保密义务，服务期满后仍需承担保密责任，直至相关信息被甲方主动公开。乙方不得泄露在提供服务时得知的与甲方业务相关的数据。（详见《项目保密协议书》）。

2.1.8 乙方在履行本合同之前，需以书面方式向甲方提供具体实施步骤和计划，在设备的使用、

信息的获取和更改方面得到甲方书面确认。乙方实施渗透测试等高风险操作前 48 小时须向甲方网络安全部门报备，并配备应急响应小组现场值守。

2.1.9 乙方将按照双方约定的实施方案中规定的时间保质保量完成指定的审核和评估内容。乙方应协助甲方通过相关主管部门的监督检查，并负责任何因自身原因导致的整改工作。乙方须协助甲方定期备份数据，确保数据完整性。发生安全事件时，乙方需立即响应并协助处理。

2.1.10 因乙方服务不当、疏忽导致的甲方损失，乙方应承担全部赔偿责任。乙方应承担因项目实施人员行为导致的法律责任和经济赔偿，并且承担因其服务导致的第三方索赔，甲方不承担任何责任。

2.1.10 关于项目周期双方协商约定如下：_____

2.1.11 以上内容乙方如有违背，甲方可以按照本合同第七章《违约责任》以及《项目保密协议书》第五条中相应条款追究乙方违约责任。

2.2 甲方职责

2.2.1 甲方将以书面形式指定一个项目协调人，以配合乙方的项目组工作，负责所有与乙方公司的正式交流，同时提供及时的信息反馈。

2.2.2 甲方将指定相关技术人员，为乙方提供进行本合同约定的信息安全服务所需要的信息。

2.2.3 甲方将提供适当的工作区，包括电话机、复印机、传真机等办公条件。

2.2.4 甲方将为乙方提供进行本合同约定的信息安全服务所需要的访问网络设备和主机设备的权限。

2.2.5 甲方将向乙方提供实施本合同约定的信息安全服务所需要的文件。

2.2.6 甲方保证拥有必要的许可、证明，确保乙方实施本合同中约定的服务时，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。

2.2.7 事先未征得乙方的同意，甲方不得转让合同的全部或任一部分。

2.2.8 甲方将按照本合同中约定的付款方式和时间付款。

2.2.9 在合同有效期内及之后的 18 个月内，甲方不得在未经乙方同意的情况下，擅自雇用乙方人员。

2.2.10 甲方应按照乙方的要求，提供信息安全服务工作所需要的相关资料，并对其合法性、真实性、合规性等承担个别及连带责任。

2.2.11 以上内容甲方如有违背，乙方可以按照本合同第七章《违约责任》以及《项目保密协议书》第五条中相应条款追究甲方违约责任。

第三章 保密条款

3.1 在本条款中，“保密信息”指：

3.1.1 甲方提供给乙方的一切非公开技术和非技术信息，包括但不限于：网络拓扑结构；业务流程；商业理念；网络安全机制；网络设备；网络方案；以及任何乙方无权向第三方泄露的信息。

3.1.2 乙方的网络安全等级测评服务流程，服务问卷，服务项目控制文档等，任何甲方无权向第三方泄露的信息。

3.1.3 无论在信息安全服务过程中和信息安全服务结束后，双方都有义务不向任何第三方泄露信息安全等级测评服务过程中所获知的保密信息。

3.2 具体保密内容以及违约责任参见本合同附件《项目保密协议书》。

第四章 协议的变更

4.1 协议的变更，需通过双方正式书面文件确认并由甲方和乙方的授权签约者共同签署后方有效。在特殊情况下，如因国家法律或政策变化、甲方职能调整等原因，甲方有权单方提出变更或解除合同且无需承担任何违约责任，乙方应予以配合。

4.2 以上条款如有未尽事宜，经甲、乙双方协商后加以补充。

第五章 付款方式

5.1 本次信息系统安全服务项目的资金总额为：￥_____元人民币（RMB￥：_____元）。

5.2 支付方式：一年一付，按每年度金额支付，金额为：_____（￥_____元），其中不含增值税的金额为￥_____元，增值税预估税额为￥_____元，增值税税率为6%，共计三年。

5.3 付款条件

付款条件	支付比例	金额（人民币：元）
甲乙双方签订合同后七个工作日内，甲方向乙方支付项目预付款	50%	￥ 元 人民币大写：
甲方在取得《信息安全等级测评报告》且经甲方验收合格后，七个工作日内向乙方支付项目款	40%	￥ 元 人民币大写：
服务期限届满后甲方在七个工作日内向乙方付清项目款	10%	￥ 元 人民币大写：

上述付款均以乙方提供相应金额的发票为前提，否则甲方有权拒不付款且不构成违约。

第六章 服务期限

服务期限：叁年，自_____年___月___日起至_____年___月___日止。乙方应在合同终止或到期时无条件配合完成服务交接，以确保业务连续性。

第七章 协议的效力

6.1 本协议由甲、乙双方共同拟定，双方均认可本协议的所有条款，并愿意为履行协议条款承担法律责任。

6.2 本协议应经双方主要负责人签字并加盖有效公章方可生效。

6.3 本合同期满后，双方应继续按照本合同有关信息保密的规定继续履行保密协议。

6.4 如果任何一方不履行合同义务，经对方一次催告后五日内未作答复并实际履行合同义务，则对方可在发出二次催告后十日内终止合同，并可按本合同第七章约定要求对方承担相应违约责任。

6.5 本协议一式 **捌** 份，甲方执 **肆** 份，乙方执 **肆** 份， 具有同等法律效力。

第八章 违约责任

7.1 如本合同因任何一方过错导致不能履行或不能完全履行，将按照以下条款支付给对方相应的违约金。

7.1.1 乙方未按照本合同约定时间提交约定的服务成果，或所提交的服务成果不符合合同约定，每延迟一天应向甲方支付合同总价款千分之五的违约金，延迟超过 15 天的，甲方有权单方解除合同，并要求乙方赔偿包括直接损失、间接损失在内的全部损失。

7.2 如果乙方违背了信息系统安全服务项目的承诺保证，甲方可以追究乙方相关责任。但是“安全是相对的，绝对的安全是不存在的”。乙方将以专业化的工作方式向甲方提供信息系统安全服务并给出审核及评估结果和信息安全建议，以增加本次项目中涉及的甲方信息系统的安全保障能力。但乙方不承诺给出的结果及建议能够完全涵盖被审核及评估信息系统的所有安全漏洞与风险；乙方也不因此承担甲方由于入侵者攻击而遭受损失的责任，但乙方对已知行业共性高危漏洞未在测评报告中披露，或因服务过程存在重大过失、未按行业标准操作导致甲方遭受损失的，应承担相应的赔偿责任。

7.3 如果甲、乙双方由于一方对合同中约定的义务履行存在过错，如没有获得必要的许可证或资质；侵犯第三方隐私；违反适用的法律法规等。由此造成的损失、债务和法律责任由该方全部承担。

第九章 不可抗力

8.1 任何一方因不可抗力而暂时无法履行合同时，将履行期限延长至该不可抗力结束后，期限与费用不变。不可抗力的定义应严格限定，不包括任何一方可预见、可控制的风险（如人员流失、技术故障等）。发生不可抗力时，相关方应立即书面通知另一方，并采取一切合理措施减轻损失，否则不得主张免责。因不可抗力导致甲方无法履行付款或配合义务的，甲方不承担违约责任。不可抗力期间，甲方有权单方解除合同且不承担任何责任。

8.2 因不可抗力致使本合同无法履行时，双方均有义务立即以电话、传真或电报等最简捷的方式尽快通知对方，并于不可抗力发生后 14 日内，以航空挂号信函寄送当地主管机构核发之证明，以证实该不可抗力之发生和存在。该不可抗力终止或排除后，应以同样方式通知对方。

8.3 不可抗力发生后，双方均有权就是否继续履行本合同进行磋商。

第十章 争议与仲裁

本合同未尽事宜由双方协商解决。协商不成的，任何一方有权向甲方所在地的人民法院提起诉讼解决。争议解决期间，除双方发生争议部分以外，本合同的其他部分仍应继续。

甲、乙双方的授权代表在下面签字，表示同意本协议的所有条款及条件。

甲方： **乙方：**

（盖 章） （盖 章）

开户银行：

账号：

签字： 签字：

签字日期： 年 月 日 签字日期： 年 月 日

第十一章 附件

附件一：项目保密协议书

根据中华人民共和国有关法律、法规，经甲乙双方协商一致，就甲方委托乙方依据《信息安全等级保护管理办法》(公通字[2007]43 号)、《信息安全技术 网络安全等级保护基本要求》、《信息安全技术 网络安全等级保护实施指南》、《信息安全等级保护安全建设整改工作指南》《风险评估实施指南》《安全加固指南》《安全运维指南》对甲方信息系统实施 （项目名称） 所涉及的保密信息（资料、数据、技术等）事宜，双方达成协议如下：

第一条 总则

一、甲、乙双方同意，在《河南省教育考试院信息系统安全服务项目合同书》的签订、履行过程中通过口头、书面、电子或其他方式知悉的对方技术、数据、报告、资料、记录等信息以及属于第三方但对方负有保密义务的信息，除该方做出相反的书面说明外，均应视为该方的秘密或商业秘密。

二、对于甲、乙双方已确认为秘密的信息均须以书面形式严格限制其仅在指定的人员或机构中流动，未经秘密信息所有方的书面同意，不得以介绍、复印、拷贝、发表文稿等方式外泄。

第二条 乙方义务

乙方所有交付成果知识产权归属甲方，未经许可不得用于其他商业用途。

一、乙方获得或知晓的甲方的秘密信息，仅用于本次项目及协商双方合作的用途。乙方不得将甲方资料用于与本项目无关的任何目的，不得以任何方式向第三方披露、转让或授权使用，并且乙方负有维护已知甲方秘密信息保密性的责任，不得向任何第三方泄漏。

二、保密条款：

a)乙方同意遵守甲方有关保密的各项管理规定。甲方有权依据上述制度对乙方进行检查。

b)未经甲方书面许可，乙方不得将所知的甲方秘密信息以任何方式提供给任何第三方。

c)未经甲方书面许可，乙方不得擅自披露甲方的秘密信息。

d)除了甲乙双方约定的工作目的之外，未经甲方书面许可，乙方不得擅自使用甲方的秘密信息。

e)未经甲方书面许可，乙方不得带走从甲方得到的任何文档、图纸、资料、磁盘、胶片等载有甲方秘密信息的介质。

f)乙方因工作需要必须携带的数据资料，须经甲方书面许可后加密或封条存储。

g)对于项目实施过程中采集到的数据、信息和服务结果的保管、访问，乙方无关人员不能访问；因工作需要必须访问的人员，乙方应进行严格的访问控制；乙方应对管理以上秘密信息的人员进行严格筛选。

h)工作期满离开时，乙方应将包含甲方秘密信息的一切资料及其复印件如数交还甲方，未经甲方书面

许可，乙方不得擅自保留。

i)乙方在项目实施过程中负有风险预估、及时预报的责任，在具有风险性的工作进行之前应向甲方说明该项工作将带来的影响。

j)未经甲方书面许可，乙方的移动设备、个人信息处理设备等不得擅自接入甲方的生产及办公网络。

k)甲方以书面形式同意乙方使用一定的资源，如网络、NOTES 等，乙方只能将其用于本次项目工作目的，不得从事任何侵害甲方利益的活动。

l)甲方以书面形式同意乙方使用的工具、技术和方法，如扫描、测试等，乙方只能将其用于本次项目工作目的，不得用来从事任何侵害甲方利益的活动。

m)乙方保证，不会利用与本次项目相关的秘密信息为自己或第三方开发信息、技术和产品，或与另一方进行商业竞争。

n)乙方承诺其所属员工对上述保密条款负有履行义务，乙方通过一定的书面手段保证上述承诺。

三、保密内容：

a)甲方的机构设置和运行机制。

b)甲方的计算机及其它辅助产品、安全产品的型号、数量、配置、运行状态等资料。

c)甲方的应用系统名称、功能、业务类型、交易量、交易特征等信息。

d)甲方的现有网络拓扑结构及其相关资料。

e)甲方的业务流程、逻辑流程等资料。

f)甲方的计算机系统的漏洞信息。

g)甲方的现有安全机制及安全系统。

h)甲方与其它单位的合作信息、合同。

i)本次信息安全等级测评项目的所有文档和资料。

j)其它经甲方确认需要保密的信息资料。

第三条　甲方义务

一、甲方获得或知晓的乙方的秘密信息，仅用于本次项目及协商双方合作的用途。并且，甲方负有维护已知乙方秘密信息保密性的责任，不得向任何第三方泄漏。

二、保密条款：

a)甲方使用乙方的资料仅用于本次信息安全等级测评项目。

b)甲方保证，对于乙方提供的资料只在直接相关人员中传阅。

a)甲方保证，不以任何方式对乙方提供的各种介质的资料进行未经授权的复印、翻译和转发；但甲方由于后续项目建设需要，对乙方所提供的资料进行节选和复制，不在本保密范围约束之列。甲方

有权在本项目及后续相关项目中合理使用乙方交付的成果、报告及相关资料，乙方不得以任何理由限制甲方的合理使用权。

b)乙方为本次项目提供的所有资料，经双方确认后，除本次项目的文档和资料外，甲方均在项目结束后交回乙方或根据其要求销毁。

三、保密内容：

a)《2025 河南省教育考试院网络安全服务项目合同书》

b)所有信息安全等级测评服务实施过程性文档，如：作业指导书、现场评测记录表、工具测试记录表等内容。

c)等级评测流程相关说明文档。

d)所有与该项目相关的项目过程控制文档。

e)其它经乙方确认需要保密的信息资料。

f)甲方承诺，其接触并知悉上述秘密信息的员工负有保密义务，甲方通过一定的书面手段保证上述承诺。

第四条 不可抗力

甲、乙双方确认，任何一方因不可抗力（如法律、法规、国家政策规定等）而必须透露对方秘密信息的，应事先以书面的形式通知对方，并且尽力为对方的秘密信息提供保护。

第五条 违规责任

一、违约的一方承担违反此协议所造成的经济损失。

二、如果违约方支付的违约金不足以补偿对方因违约方违反本协议而遭受的其他损失，违约方应当继续承担赔偿责任。

三、违约方违反本保密协议，给对方造成的损失额以下面两种方法计算的较高者为准：

a)以对方因被侵害而受到的实际损失作为赔偿额。

b)以违约方因违约所获得的全部收益作为赔偿额，包括违约方将该秘密信息泄露给第三方，第三方因此而得到的收益。

四、因违约方的行为造成对方的秘密信息完全公开的，违约方应赔偿该秘密信息的全部价值，同时违约方应承担信息泄密后相应的法律责任。

第六条 协议变更与补充

一、本协议履行过程中，双方经协商一致，允许对本协议进行变更。变更均须以书面形式提出，由甲乙双方签字确认。

二、本协议如有未尽事宜，须经双方共同协商并达成书面补充协议，补充协议与本协议具有同等法律

效力。

第七条 适用法律及合同争议解决

一、本协议适用中华人民共和国法律。

二、因本协议引起的任何争议，双方应首先尝试通过协商解决。不能达成争议解决协议的，则任何一方有权向甲方所在地人民法院起诉。

三、在诉讼期间，本协议不涉及争议的条款仍须履行。

第八条 协议的生效

本协议作为《河南省教育考试院信息系统安全服务项目合同书》的附件，自甲乙双方法定代表人（负责人）或授权代理人签字并加盖公章后生效。

第九条 双方约定的其他事项

本协议作为《河南省教育考试院信息系统安全服务项目合同书》的附件，是该合同不可分割的组成部分。如本协议内容与该合同正文存在冲突之处，则以该合同正文内容为准。

需 方：	供 方：
盖 章：	盖 章：
代 表：	代 表：
地 址：	地 址：
邮政编码：	邮政编码：
电 话：	电 话：
开户单位：	开户单位：
签订时间：	签订时间：

第五章 项目需求

1.项目概述

1.1.项目背景

当前，网络空间安全面临的形势复杂多变，对抗趋势越发凸显。以窃取敏感数据破坏关键信息技术设施为目标有组织的网络攻击愈演愈烈，零日漏洞、供应链攻击、数据泄露等重大安全事件层出不穷。近年来国家不断完善网络空间安全顶层设计，《网络安全法》《数据安全法》《密码法》《关键信息基础设施安全保护条例》等法律法规的出台，对网络安全运维建设提出了明确要求。因此，为持续满足国家网络安全要求，加强网络安全风险控制措施的落实，采购方需建立一套“平战融合”的实战化网络安全运维体系，通过高效协同的梯队式安全服务团队，采用规范化的运维管理，按照标准化、流程化的安全运维机制开展可信、可控和可量化的高质量安全运维服务，以整体提升采购方网络安全保障能力。

1.2.项目目标

本项目以贯彻《中华人民共和国网络安全法》等国家网络安全和信息化基本法规制度为依据，以落实采购方网络安全和信息化的“四统一、五集中”工作要求为指导,以提高采购方网络安全运维能力为核心目标，以整合网络安全、云安全、终端安全、移动安全、网站安全等各类安全运维服务为基本措施，通过提供“互联网监控-常态化驻场服务-专项安全治理服务”的立体化服务，实现对网络威胁“安全预测、威胁防护、持续检测、响应处置”的安全风险管控，构建基于平战融合的实战化网络安全运维体系，确保采购方的网络安全体系高质量健康发展，同时，不断提升网络安全对抗能力，做好关键时期的网络安全保障工作，促进网络安全综合防护能力与水平持续提升。

落实采购方网络安全运行管理制度，规范运行维护流程，形成较为完善的运行维护管理体系。加强网络安全运行保障、监控预警能力建设，依托专业化运维队伍，对云、网络、计算、存储、基础软件、安全设备等网络安全基础设施实施统一运维，实现系统快速部署更新、资源合理高效调度、网络实时动态监控和安全稳定可靠，有效降低运维经费成本，提高运维服务质量和水平。建立集中统一的信息安全保障机制，落实信息安全等级保护、分级保护等国家信息安全制度，开展信息安全等级测评、风险评估安全防范、应急处置等工作。加强网络安全建设，构建环保云安全管理中心，增强大数据资源和应用系统等的安全保障能力。

1.3.主要依据

依据《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》(国务院第147 号)、《中华人民共和国密码法》《中华人民共和国个人信息保护法》等相关法律要求，确保信息

系统安全等级保护工作符合国家法律框架。遵循《关于印送<贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见>的函》（公安部 1960 号文）、《河南省计算机信息系统安全保护暂行办法》(河南省人民政府令 第 53 号)、《信息安全等级保护管理办法》(公通字[2007]43 号)等具体规定，进行等级保护的实施和管理。深入贯彻《教育部关于印发<教育行业信息系统安全等级保护定级工作指南>的通知》(教技厅函[2014]74 号)、《教育部公安部关于全面推进教育行业信息安全等级保护工作的通知》(教技[2015]2 号）和《河南省教育厅、河南省公安厅关于深入开展教育行业信息系统安全等级保护工作的通知》(教科技[2015]710 号）等信息系统安全和网络安全等级保护制度的相关标准规范和要求，为测评工作提供具体的测评方法和要求。

遵守《中华人民共和国保守国家秘密法》，遵守采购方要求的保密规定及工作纪律，签订保密协议并履行保密责任；服务单位工作人员与服务单位签订保密协议，其行为由服务单位进行约束并承担责任。

1.4.项目内容

采购方网络安全服务内容主要包括采购方各项招生考试业务信息系统的等级保护测评，全院所有网络设备、安全设备、服务器及终端的日常安全巡检、定期漏洞扫描，各项招生考试业务信息系统上线前的源代码安全检测，各项招生考试业务信息系统的定期漏洞扫描、风险评估、渗透测试及安全加固，日常办公运维、内网安全态势监测与分析、互联网暴露面安全监测与分析、重点业务安全保障、专项安全治理、网络攻防演习、安全管理人员的专业技能培训和全院办公人员的安全技术及意识培训等，囊括采购方动态的、整体的安全管理和保障体系的建立。

安全服务工作内容表

序号	服务项目	服务内容	服务地点
1	等级保护测评服务	等级保护测评服务	郑州、登封
2		等级保护备案服务	郑州、登封
3		等级保护整改服务	郑州、登封
4		网络安全等级保护综合服务平台	郑州、登封
5	互联网暴露面安全监测与分析服务	互联网资产发现	郑州、登封
6		自动化渗透测试	郑州、登封
7		网站安全监测	郑州、登封
8	内网安全态势监控与分析服务	提供流量采集工具与分析工具	郑州、登封
9		人工监控与分析	郑州、登封
10	源代码检测	应用代码审计	郑州、登封

11	渗透测试	应用渗透测试	郑州、登封
12	漏洞扫描	提供专业的漏洞扫描工具	郑州、登封
13		定期进行漏洞扫描	郑州、登封
14	安全加固与补丁服务	基础安全检查	郑州、登封
15		策略梳理与加固	郑州、登封
16		服务器安全加固	郑州、登封
17		虚拟机模板加固服务	郑州、登封
18		补丁提供服务	郑州、登封
19	重点业务保障安全服务方案	重保现场安全值守	郑州、登封
20		重点业务工作保障	郑州、登封
21	日常办公网络安全运维服务	网络安全运维	郑州、登封
22		终端安全运维	郑州、登封
23		安全通报	郑州、登封
24		资产管理	郑州、登封
25	专项安全治理服务	数据泄漏排查	郑州、登封
26		勒索、挖矿病毒排查	郑州、登封
27		弱口令清查	郑州、登封
28	网络和数据安全行业监管服务平台服务	网络和数据安全行业监管服务平台	郑州、登封
29	定制开发服务	根据采购方需求对安全设备或系统的功能进行定制开发	郑州、登封
30	应急响应服务	应急预案	郑州、登封
31		应急响应	郑州、登封
32	应急演练服务	应急演练筹备、演练、总结、整改	郑州、登封
33	网络安全攻防演习	网络安全攻防演习	郑州、登封
34	数据管理能力成熟度评估服务	数据管理能力成熟度评估服务	郑州、登封
35	安全培训服务	安全意识培训	郑州、登封
36		安全攻防培训	郑州、登封

采购方安全服务设备列表

序号	设备类型	应用	数量
1	服务器	WEB 服务器	17 台
2		FTP 服务器	2 台
3		MAIL 服务器	1 台
4		应用服务器	37 台
5		数据库服务器	17 台
6		网上阅卷服务器	150 台
7	安全设备	防病毒系统	1 套
8		CFCA SSL 通配域名	1 套
9		IPS 入侵检测	2 台
10		防火墙	6 台
11		WAF 防火墙	4 台
12		VPN	2 台
13		动态防护	3 台
14		数据库审计系统	5 台
15		堡垒机	5 台
16		准入控制	1 台
17		CA	1 套
18		RA	1 套
19		签名验签	1 套
20		密码机	1 台
21		上网行为管理	1 台
22		综合威胁探针	2 台
23		安全隔离网闸	2 台
24		日志审计系统	3 台
25		主机安全	1 台
26		数据库备份与恢复系统	4 台
28	终端	PC 机器	480 台

2.项目服务需求

为保障采购人网络安全稳定运行，投标人必须提供本次招标文件所列出的所有服务和工具，并按要求提供相关证明材料，如果未能满足，投标将被拒绝且不允许在开标后补证。

本项目需提供 5X8 小时的驻场服务，7X24 小时的应急响应服务，建立应急响应机制。在非驻场时间接到采购方应急响应需求后,指派专业工程师 1 小时内到达现场，并快速解决问题，在“全国两会和重要业务时间节点”等重要时期，提供重保服务。

2.1.等级保护测评服务

信息系统安全等级保护测评项目的范围涉及采购方以下信息系统：

等级保护测评系统表

序号	信息系统名称	信息系统描述
1	河南省招生考试考生服务平台	招生考试业务考生信息网上填报系统
2	河南省招生考试网上录取系统	招生考试业务网上录取系统
3	河南省招生考试信息网络管理系统	招生考试业务考试信息网络管理系统
4	采购方门户网站	采购方门户

信息系统安全等级保护测评项目的具体实施范围及实施时间由采购方确定。

2.1.1.测评依据

投标人提供的服务必须符合下列标准和规范的最新版本，但不限于此：

GB/T 20984-2007：《信息安全技术 信息安全风险评估规范》

GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》

GB 17859-1999：《信息安全技术 计算机信息系统安全保护等级划分准则》

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

GB/T 25058-2019：《信息安全技术 网络安全等级保护实施指南》

GB/T 28448-2019：《信息安全技术 网络安全等级保护测评要求》

GB/T 22240-2020：《信息安全技术 网络安全等级保护定级指南》

T/ISEAA 001-2020：《网络安全等级保护测评高风险判定指引》

2.1.2.工作内容

信息系统定级及备案。根据系统分类和梳理的结果，协助采购方完成信息系统的备案及备案变更服务。

信息系统等级保护测评。根据采购方信息系统的保护等级，按照相关标准逐一对信息系统的安全保护等级进行测评。并出具符合国家要求的信息系统等级测评报告和整改建议。

2.1.3.施工要求

信息系统测评及备案

按照国家信息安全等级保护相关标准要求，对采购方相关信息系统实施等级保护测评活动，并出具符合国家要求格式的《网络安全等级测评报告》，且在测评工作完成后协助采购方完成相关信息系统的备案或备案变更工作。

测评工作应依据等级保护 2.0 基本要求相关内容组织开展，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、安全管理制度、安全管理机构、安全管理人员、安全

建设管理、安全运维管理十个层面的测评并进行综合分析，得出整体结论，形成等级测评报告。具体内容如下：

等保测评控制表

安全类	安全控制点	测评内容
安全物理环境	物理位置选择	重点测评机房场地的选择及其防震、防风和防雨等能力等。
	物理访问控制	重点测评机房出入口访问控制、鉴别和记录能力等。
	防盗窃和防破坏	重点测评应将设备或主要部件固定、标识，通信线缆铺设，机房防盗报警措施等。
	防雷击	重点测评各类机柜、设施和设备接地措施，防止感应雷措施等。
	防火	重点测评机房火灾消防措施，机房及相关的工作房间和辅助房建筑材料耐火等级，区域隔离防火措施等。
	防水和防潮	重点测评防止雨水渗透措施，防止机房内水蒸气结露和地下积水的转移与渗透措施，防水检测和报警措施等。
	防静电	重点测评接地防静电措施以及采取措施防止静电的产生等。
	温湿度控制	重点测评温湿度自动调节设施。
	电力供应	重点测评机房供电线路稳压措施，短期的备用电力供应措施，冗余计算机系统供电措施等。
	电磁防护	重点测评线缆隔离铺设和关键设备电磁屏蔽措施。
安全通信网络	网络架构	重点测评网络设备的业务处理能力，网络区域划分、地址分配，重要网络区域技术隔离手段，通信线路、关键网络设备和关键计算设备的硬件冗余等。
	通信传输	重点测评通信过程中数据的完整性和保密性控

		制措施。
	可信验证	测评是否基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。
安全区域边界	边界防护	重点测评跨越边界的访问和数据流通信受控情况，非授权内联、外联的检查或限制措施，无线网络的使用和控制措施等。
	访问控制	重点测评网络边界或区域之间访问控制规则，访问控制列表优化，并保证访问控制规则数量最小化；是否基于应用协议和应用内容对进出网络的数据流实现访问控制等。
	入侵防范	重点测评关键网络节点检测、防止或限制从外部或内部发起的网络攻击行为的能力，网络攻击行为分析、记录及报警措施等。
	恶意代码和垃圾邮件防范	重点测评在关键网络节点处对恶意代码进行检测和清除，以及对垃圾邮件进行检测和防护的能力。
	安全审计	重点测评在网络边界、重要网络节点的安全审计措施，审计覆盖范围、审计记录详细程度、审计记录保护措施，远程访问的用户行为、访问互联网的用户行为审计和数据分析措施等。
	可信验证	测评是否基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证。
安全计算环境	身份鉴别	重点测评终端、服务器、网络等设备中的操作系统的登录用户身份标识和鉴别措施。
	访问控制	重点测评终端、服务器、网络等设备中的操作系统的登录用户的账户分配和权限管控措施。
	安全审计	重点测评终端、服务器、网络等设备中的操作系统的安全审计功能，审计覆盖范围、审计记录详

		细程度、审计进程保护措施。
	入侵防范	重点测评终端、服务器、网络等设备中的操作系统是否遵循最小安装的原则，管理终端访问限制措施，数据有效性检验功能，已知漏洞测试、评估、修补，重要节点入侵检测及报警措施等。
	恶意代码防范	重点测评是否采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为并有效阻断。
	可信验证	重点测评是否基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。
	数据完整性	重点测评是否采用校验技术或密码技术保证重要数据在传输、存储过程中的完整性。
	数据备份恢复	重点测评重要数据的本地数据备份与恢复功能，异地实时备份功能，重要数据处理系统的热冗余措施。
	剩余信息保护	重点测评鉴别信息或敏感数据所在的存储空间被释放或重新分配前是否得到完全清除。
	个人信息保护	重点测评是否仅采集和保存业务必需的用户个人信息，是否禁止未授权访问和非法使用用户个人信息。
安全管理中心	系统管理	重点测评中心系统管理员身份鉴别和访问控制措施，中心系统管理员对系统的资源和运行进行配置、控制和管理能力等。
	审计管理	重点测评中心审计管理员身份鉴别和访问控制措施，中心审计管理员对审计记录的分析、存储、管理和查询能力等。
安全管理制度	安全策略	重点测评是否制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

	管理制度	重点测评各类安全管理制度建设情况以及各类系统操作规范建设情况。
	制定和发布	重点测评安全管理制度制定的责任部门设立情况；安全管理制度的制定过程以及发布方式。
	评审和修订	重点测评安全管理制度评审修订时机以及目前安全管理制度修订情况。
安全管理机构	岗位设置	重点测评安全管理岗位设立及职责明确情况。
	人员配备	重点测评安全管理岗位人员配备情况。
	授权和审批	重点测评针对重大系统操作的授权和审批情况。
	沟通和合作	重点测评与系统内部以及外部相关部门、单位的日常沟通机制。
	审核和检查	重点测评系统安全检查工作规范化程度和落实情况。
安全管理人员	人员录用	重点测评人员录用过程规范化管理；对录用人员保密责任的约束方式以及对关键岗位职责约束的方式。
	人员离岗	重点测评人员离岗过程控制；人员离岗的保密承诺控制。
	安全意识教育和培训	重点测评安全培训计划的制定情况和实施情况。
	外部人员访问管理	重点测评对外部人员进入重要区域的审批、控制管理。
安全建设管理	定级和备案	重点测评网络系统是否明确其安全保护等级，系统定级、审批及备案的相关情况。
	安全方案设计	重点测评系统的网络安全工作的总体规划设计情况。
	产品采购和使用	重点测评系统中网络安全产品、密码产品和服务的采购和使用管理措施。
	自行软件开发	重点测评系统内自行软件开发工作的管理和控制措施。
	外包软件开发	重点测评外包软件开发的安全管控措施。

	工程实施	重点测评网络系统工程的实施过程的安全管控措施。
	测试验收	重点测评网络系统工程的安全验收措施。
	系统交付	重点测评网络系统工程的系统交付安全管控措施。
	等级测评	重点测评网络系统等级测评工作开展情况。
	服务投标人选择	重点测评对系统中相关的安全服务商选择以及服务管理措施。
安全运维管理	环境管理	重点测评对机房基础设施日常管理情况以及办公环境的管理。
	资产管理	重点测评对系统资产管理的制度建设情况以及标识管理。
	介质管理	重点测评对各类介质的传输、使用、存储和销毁等环节的管理。
	设备维护管理	重点测评对各类设备日常的使用、操作和维护维修的管理。
	漏洞和风险管理	重点测评安全漏洞和隐患发现，漏洞和安全问题修补管理措施。
	网络和系统安全管理	重点测评网络和系统日常安全管理措施。
	恶意代码防范管理	重点测评对恶意代码的检测、分析等防范工作的管理。
	配置管理	重点测评各个设备或软件组件的基本配置信息保存措施，以及信息变更控制措施。
	密码管理	重点测评密码技术和产品的使用和管理情况。
	变更管理	重点测评变更活动制度化建设情况以及变更前、变更中和变更后的规范化管理情况。
	备份与恢复管理	重点测评系统数据的日常备份管理以及系统恢复管理。
	安全事件处置	重点测评安全事件报告和处置的制度建设情况以及不同安全事件处理过程的规范化管理

		情况。
	应急预案管理	重点测评应急预案制定情况、人力、设备、技术、财务和外部协作等方面的资源保障情况以及对应急预案的培训和日常演练情况。
	外包运维管理	重点测评外包运维商的选择和安全管控措施。

系统整体测评

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。应包括如下方面的整体测评：

（a）安全控制间安全测评：安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。

（b）层面间安全测评：层面间的安全测评主要考虑同一区域内的不同层面之间存在的功能增强、补充和削弱等关联作用。

（c）区域间安全测评:区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

2.1.4.网络安全等级保护综合服务平台服务

投标人基于测评机构特有的行业优势，在等级保护测评服务结束后，需为采购方提供一套网络安全等级保护综合服务平台。平台定位于网络安全等级保护工作全阶段全过程管理，覆盖了信息系统定级、备案、等级测评、安全建设整改等工作环节，通过平台可全面梳理等保工作各项内容，描摹系统安全画像，推进等级测评、安全建设整改、监测预警、应急响应等事项落实。

交付成果：《网络安全等级保护等级测评报告》、协助用户方完成被测系统的备案及备案变更服务、部署网络安全等级保护综合服务平台。

服务频次：服务期内被测系统等保测评服务为每年 1 次，网络安全等级保护综合服务平台部署完成。

2.2.互联网暴露面安全监测与分析服务

2.2.1.互联网资产发现

根据采购方实际安全需求，每季度使用专业的互联网资产发现工具对采购方对外发布的信息的IP、域名进行互联网资产发现测试，发现采购方互联网侧的主机服务器、安全设备、网络设备、WEB 应用、中间件、数据库等已知/未知资产或资产变更，及时更新资产台账。

互联网资产发现服务工作内容应包括:

绘制信息安全资产底图:通过使用互联网资产发现工具，生成采购方专属的信息安全资产画像，构建专属的安全资产底图。

资产及应用发现:通过使用互联网资产发现工具自动发现采购方服务器、安全设备、WEB 应用、中间件、数据库、邮件系统和 DNS 系统等资产，并生成资产列表。

资产分布情况评估:通过使用互联网资产发现工具按归属地、责任人、部门等条件，对采购方资产分布情况进行评估。

2.2.2.安全监测与分析

另外还需提供专业的网站安全监控平台供采购方使用,平台应具有专业扫描引擎和高质量漏洞库，具备仿真算法高交互深度分析功能，能全面精准发现网站潜在的漏洞和安全问题，平台具备针对考试院两网两微等业务进行 7x24 小时安全监测能力，同时提供相应的后期分析与研判的人工服务。

(一)监控预警平台可对常见的门户网站以及业务系统提供以下11种常见网站安全事件的监测告警服务：

1)可用性监测服务（HTTP、DNS、PING）

2)远程网页变更监测服务

3)远程网页敏感信息监测服务

4)远程网页恶意链接监测服务

5)Web漏洞扫描检测服务

6)主机系统漏洞扫描服务

7)网站钓鱼检测服务

8)网页木马检测服务

9)弱口令检查检测服务

10)WebShell检测服务

11)安全威胁情报

定期针对监控到的安全问题进行分析与研判，确认安全问题的真实性和影响性以及提供相应的解决方案。

交付成果：《安全监测表》、季度《互联网资产发现报告》

服务频次：平台实时安全监测、互联网资产发现每季度 1 次。

2.3.内网安全态势监控与分析服务

投标人需提供基于全流量采集和分析的专业工具包括但不限于 APT、态势平台、日志审计等工具，分析采购方网内安全威胁，利用威胁情报数据，利用采集到的安全大数据并采用专业攻防思路构建分析模型，提供内部失陷主机、外部攻击、内部违规和内部风险等关键信息安全问题的周期性的检测、发现和响应服务，包括但不限于数据库威胁操作分析、WEB 攻击分析、服务器被攻击行为分析、异常外联分析、资产梳理分析、非常规检测分析、账户风险分析、邮件安全分析等。及时发现潜在的安全威胁，对威胁的恶意行为实现快速发现，对受害目标及攻击源头进行精准定位，对入侵途径及攻击者背景的研判与溯源，减少安全威胁带来的损失。

监控与分析平台需具备：

1)★安全探针：专业 APT 等类型分析设备，可以提供 10G 的流量分析能力。

2)★分析平台：专业硬件设备，全面兼容采购方现有安全设备，无缝对接能力。

3)数据库行为分析:检测内容包括数据库的内置高危存储过程识别、数据库敏感操作识别、数据库目录遍历、权限提升、非常规操作识别等;

4)Web 攻击分析:检测内容包括 Web 通用弱口令检测识别、弱口令爆破成功识别 Webshell 存在识别、Web 漏洞扫描识别、黑产后门扫描识别、SQL 注入攻击识别 Struts2 攻击识别、上传行为攻击识别、敏感信息泄露识别、XSS 跨站攻击识别、敏感路径访问识别等;

5)登录行为分析:检测内容包括主动式弱口令探测、基于相关信息生成口令、暴力破解识别、被动式邮件、WEB 等弱口令探测、通用默认密码检测等;

6)服务器危险行为分析:检测内容包括反弹 shell 识别、Redis 命令执行识别、DNSTunnel 检测、反序列化攻击检测、其他高危漏洞等:

7)非法外联分析:检测内容包括非法外联行为识别、SSH 隧道外联行为识别、基于情报的外联行为识别;

8)内部资产梳理:检测内容包括资产类型、开放服务及端口识别、资产 Web 应用识别、资产 Web 中间件识别、资产 Web 业务类型识别、资产 Web 开发语言识别、资产应用绑定域名识别、资产外联分析等;

9)邮件行为分析:检测内容包括邮件安全策略检测(SPF)、钓鱼邮件检测、恶意附件检测、敏感邮件内容检测等;

10)数据库行为分析:检测内容包括数据库的内置高危存储过程识别、数据库敏感操作识别、数据库目录遍历、权限提升、非常规操作识别;

11)非常规检测分析:检测内容包括 RegeoryTunnel 识别、HTTP 代理识别、SOCKS 代理识别、TeamView/IRC 识别、非标准端口分析;

12)威胁情报告警分析:检测内容包括威胁情报(IOC)告警分析、WEBIDS 告警分析。

交付成果:《网络安全威胁分析研判报告》

服务频次:服务期内平台 7*24 小时，人工按需。

2.4.源代码审计服务

为切实执行“同步规划、同步建设、同步运行”的安全工作原则，针对采购方指定的若干业务系统的上线、变更、升级改造等，采用代码审计工具和人工的方式对业务系统进行源代码安全检测，发现源代码中的弱点和错误信息，分析并找到这些弱点引发的安全漏洞，及时对漏洞进行修复，减少系统由于开发问题造成的安全隐患。投标人须自带代码审计设备完成该项工作。

代码审计的内容包括但不限于以下内容：

1. 安全漏洞检测：通过静态代码分析和动态代码测试，对软件代码进行全面的安全漏洞检测，包括常见的跨站脚本攻击、SQL 注入、代码注入、拒绝服务攻击等安全漏洞，以及对密码安全、会话管理、权限控制等方面的审计。

2. 性能问题分析：对代码进行性能分析，包括代码执行效率、内存占用、并发性能等方面的评估，发现潜在的性能瓶颈和优化空间，提高软件的性能和响应速度。

3. 代码质量评估：对代码的结构、规范性、可读性、可维护性等方面进行评估，发现代码中的潜在缺陷和不规范之处，提出改进建议，以提高代码的质量和可维护性。

4. 第三方组件审计：审计软件中使用的第三方组件和开源库，检查其安全性和可靠性，防止因第三方组件漏洞而导致的安全风险。

5. 合规性审计：审计代码是否符合相关的法律法规和行业标准，包括隐私保护、数据安全、网络安全等方面的合规性要求。

投标人应严格按照应用代码审计流程开展审计工作，在审计前期应做好应审计范围、审计对象、审计要求的确认工作;在审计中期使用自研的代码审计工具开展审计工作并做好人工审核:在审计后期应输出审计结果并汇报。

交付成果:《应用系统代码检测报告》

服务频次:服务期内按需。

2.5.渗透测试服务

在采购人的授权和监督下，中标方根据采购人的安排，采用各种手段模拟真实的安全攻击对采购方相关业务系统开展渗透测试服务，查找应用系统存在的安全隐患，并针对安全隐患提出解决办法及加固措施，切实保证业务系统安全。同时，根据业务系统漏洞修复的情况持续开展渗透测试复测工作。

投标人提供的渗透测试服务应从网络层、系统层、应用层渗透开展，并且要规避相关的网络安全风险。应与采购方签订相应的安全保密协议，确保信息、数据的泄露。

交付成果:《应用系统渗透测试报告》

服务频次:服务期内按需。

2.6.漏洞扫描服务

每季度对采购方业务系统所涉及的若干资产开展安全漏洞扫描，重点针对操作系统、数据库、中间件、网络设备和安全设备等进行安全漏洞扫描，形成扫描报告，编制修复方案，协助系统厂商完成漏洞修复。

漏洞检测工具应能对业务系统进行覆盖面广泛的安全漏洞查找，真实、全面地反映业务系统涉及的主机、网络设备、安全设备以及 Web 页面所存在的安全问题和面临的网络安全威胁。

开展漏洞检测服务应遵循严格的检测流程，需涵盖检测申请、执行检测、编制检测报告以及协助安全整改。

在进行漏洞检测过程中，应采取必要的安全风险与应对措施(如拒绝使用 DDoS 攻击、做好备份、规定检测时间段等)，避免系统宕机等。

交付成果:《漏洞检测报告》

服务频次:服务期内每季度 1 次。

2.7.安全加固与补丁服务

2.7.1.基础安全检查与加固

投标人应根据采购方的安排对所有业务系统进行安全基线检查，重点满足等保三级要求，形成网络安全基线检查报告并协助采购方整改加固。核查工作内容应包括:

●核查范围确定:在核查之前，对需要核查的资产范围进行确定，明确资产清单等

●核查工具准备:针对核查范围内的资产情况，投标人应准备相应的核查表单和利用脚本工具等。

●人工检查执行:在安全管理员的配合下，核查人员对系统进行技术检测，发现其存在的安全配置缺陷和漏洞，并对系统进行验证。

●核查报告编写:根据核查实际结果，编写相应的安全核查报告，并提出整改建议

2.7.2.策略梳理与加固

投标人应根据采购方的安排定期和不定期为其提供策略梳理服务,通过策略梳理(包括优化重复策略、无效策略、合并策略等)减少安全设备的垃圾策略再生，有效提高安全设备性能，充分发挥安全设备效能。策略梳理服务的内容应包括:

梳理采购方对安全设备的使用需求;

梳理采购方现有安全设备在网络中的部署位置、设备功能及作用:

梳理采购方现有安全设备策略的配置情况以及策略是否生效等:

分析采购方现有安全设备的种类是否满足需求;

分析采购方现有安全设备的部署位置、功能等是否满足功能要求;

分析采购方现有安全设备的策略是否满足安全要求等。

策略梳理服务的服务范围应包括采购方网络中现有安全设备及具备安全功能的网络设备。

2.7.3.服务器安全加固

在重要业务或重大活动前期应提供800点的服务器安全加固,服务器安全加固工具应支持Windows及Linux双操作系统，对操作系统的核心资源，如注册表、网络连接、系统文件、进程等进行有效防护。同时，应具备网络层攻击防护功能，发现并抵御 SQL 注入、XSS 跨站、洞利用、病毒、木马、后门等黑客入侵行为。在演习过程中，安全专家利用该工具对服务器进行实时安全监测、分析，对发现的安全问题及时上报用户。

2.7.4.虚拟机模板加固

为采购方虚拟机模板提供安全加固服务，针对虚拟机模板自身可能存在的安全漏洞和安全设置问题，提供安全加固解决方案，完成安全加固操作，尽量减少因虚拟机模板自身安全问题而产生的安全风险和隐患，每季度进行一次加固更新。投标人在开展虚拟机安全加固时，需考虑以下几方面:

●最小原则:最小服务和组件;

●最小账户:严格账户管理，对账户的增、删、改进行控制;

●最小权限:降低服务、账户以及群组的权限，对资源进行控制;

●审计控制:开启审计功能，对各类行为进行审计。

2.7.5.补丁提供服务

针对采购人无法获取的补丁，投标人应提供相关安全补丁并协助采购人安装使用。补丁类型包括但不限于 Weblogic、Struts2、jboss、Tomcat、Windows、Linux 漏洞补丁。

2.7.6.安全加固风险控制

在安全加固之前应提供详细的加固方案和风险应对措施方案，经采购方确认后方可实施。

如果在没有采购方相关人员签字确认的情况下，投标方工程人员擅自进行加固，投标方承担由于安全加固导致的一切风险。

交付成果:《虚拟机模板加固记录表》《补丁修补记录单》《服务器安全加固记录单》《策略梳理服务报告》《基线安全核查和加固报告》

服务频次:服务期内按需。

2.8.重点业务保障安全服务方案

在春节、重要会议、重大活动、黄金周长假、重要业务期间等对安全运行要求较高的特殊时段，加强驻场和二线人力保障，安排安全服务人员为采购方提供 7x24 现场值守，合理使用安全设备，对系统的安全状态进行监控，及时发现正在发生的安全事件以及潜在的安全风险，并及时定位问题，处理问题，全方位保障网络安全运行。

2.8.1.时间要求

普通高校招生考试业务服务周期为 4-6 个月

成人高校招生考试业务服务周期为 2-3 个月

研究生考试业务服务周期 1 个月

所有招生考试业务阅卷和评卷服务周期为 1-2 个月

其它招生考试业务活动等

要求中标方可根据采购方需要随时在服务期内延长服务时间

2.8.2.重保现场安全值守

在重保时期，按照采购方实际安全防护需求，做到“事前评估检查，事中监测防护，事后应急处置”。其中，事前评估检查应对指定系统开展安全漏洞扫描、基线配置核查(包括网络及安全设备基线核查、操作系统核查、数据库核查、Web 服务器和中间件核查等)以及渗透测试等工作;

事中监测防护提供安全服务人员现场驻守采购方负责实时监测攻击态势检测、分析和研判攻击事件，协助采购方进行现场调度、应急处置等工作。其监测分析内容包括:数据库行为监测和分析、恶意邮件行为监测和分析、Web 攻击行为监测和分析、非常规行为监测和分析、DNS 服务器监控、登录行为监测和分析、服务器危险行为监测和分析、非法外联行为监测和分析等。

事后应急处置应对安全事件快速处置，投标人应建立应急响应小组，7X24 小时待命应急。项目经理、驻场运维人员、二线专家手机应全天候开通，提供 7X24 小时电话技术支持，随时准备现场处理各种突发事件。

2.8.3.重要业务工作保障

重要业务保障表

服务类别	主要服务范围
各项考试业务工作中重大录取现场安全服务	1)录取工作现场安全状况监控
	2)录取现场现有安全设备的升级、安装调试与维护
	3)录取现场线路监控
	4)应急响应预案
	5)录取现场网络设备以及服务器运行状态监控
	6)录取现场系统环境的搭建
	7)录取现场工作现场的终端安全维护
	8)录取现场安全环境建设
	9)录取现场业务系统技术支持与协助
	10)录取现场招生考试业务系统信息安全培训
	11)依招标要求免费提供部分录取工作需用的安全设备及工具
各项考试业务扫描及评卷现场服务	1)扫描及评卷现场安全状况监控
	2)扫描及评卷现场现有安全设备的升级、安装调试与维护
	3)扫描及评卷现场线路监控
	4)扫描及评卷应急响应预案
	5)扫描及评卷网络设备以及服务器运行状态监控
	6)扫描及评卷现场系统环境的搭建
	7)扫描及评卷现场工作现场的终端安全维护
	8)扫描及评卷现场安全环境建设
	9)扫描及评卷现场业务系统技术支持与协助
	10)扫描及评卷现场招生考试业务系统信息安全培训
	11)依招标要求免费提供部分扫描及评卷工作需用的安全设备及工具

交付成果:《重保值班记录》《重保服务记录》《网络安全事件报告单》

服务频次：根据采购人工作需要定义的重保时间。

2.9.日常办公网络安全运维服务

2.9.1.时间要求

对办公网的运维要求投标单位提供全年不间断的派驻人员服务

可根据采购方实际工作需求在指定时间、指定地点进行服务

可根据采购方实际工作需求加班和延长服务时间

2.9.2.网络安全运维

2.9.2.1.日常安全巡检

为保障安全设备运行的连续性，投标人需提供专业的运维平台供需方使用，驻场运维人员需每天通过运维平台检查在用安全设备的运行状态(包括 CPU 利用率、内存利用率、磁盘利用率等)，及时发现安全设备运行状态异常的情况。

驻场运维人员每月对在用安全设备进行一次彻底巡检，现场检查设备状态、运行情况，远程登录设备检查设备状态指标、策略和配置并做好巡检记录，发现问题及时处置，及时对安全设备的各类特征库进行升级。建立并维护采购人安全设备资产台账。日常安全巡检内容包括:

安全设备:设备硬件状态巡检、设备软件状态巡检、设备性能状态巡检、安全策略变更、日志检查、规则库检查等

主机巡检:主机硬件状态巡检、主机操作系统安全检查、主机性能检查、可疑服务进程检查、病毒检查。

2.9.2.2.策略变更服务

落实采购人提出的安全策略调整方案，为安全设备提供配置、策略调整服务。通过全面落实安全策略、合理配置安全设备防护规则，对来自各网络区域的网络攻击行为进行阻断，通过日常的策略配置使安全防护有效发挥作用，并配合实施人员完成新部署安全设备的安装调试。

对安全设备的策略和配置进行备份操作，保证安全设备的稳定运行，在出现故障时及时恢复，保证安全防护水平。为安全设备提供配置、策略调整、备份服务。具体工作内容应包括:

策略配置:分析业务系统实际安全需求和安全设备功能，对在用安全设备的安全策略进行配置，配置过程遵循策略配置流程，对策略需求进行严格审核。

策略变更:根据采购人的安全策略调整方案，对在用安全产品的策略配置进行梳理，及时发现策略缺失、策略冗余、策略未废止等问题，加强对冗余策略和废弃策略的管控，每年进行一次。

备份恢复:每月应对在用安全设备的策略和配置进行备份，保证安全产品的稳定运行，并对备份操作进行记录。在出现故障时及时恢复，不会严重影响安全防护水平。

2.9.2.3.驻场监测分析

驻场运维人员利用已部署的防护、监测类设备和投标人提供的专业安全事件监控与分析平台，开展全年 5X8 小时的网络攻击告警监测、分析，查看网络流量情况，汇总统计网络流量趋势。

监测分析内容包括:

恶意邮件、敏感关键字邮件、钓鱼邮件、勒索邮件、诈骗邮件等的检测;

MySQL、SQL Server、Oracle 等恶意攻击行为检测;

Regeory Tunnel 隧道、HTTP 代理、SOCKS 代理等非常规服务检测;

弱口令、暴力破解、异常登录等的检测;

反弹 shell 行为、Redis 命令执行行为、反序列漏洞利用行为等的检测;

Web 攻击行为的检测分析。

负责该项工作的驻场运维人员应具有丰富的安全事件监测分析、处置能力，可对安全告警进行深入分析。

2.9.2.4.网络异常排查

在采购方的基础网络、应用系统等出现异常(如安全设备故障、网络故障无法上网、部委省厅访问专网应用异常、互联网发布异常等)时，驻场运维人员应提供网络异常排查服务。针对现有的安全设备和策略进行安全相关排查工作,积极配合网络运维系统运维等处理安全故障,以便迅速分析网络或系统异常原因,在最短时间内恢复正常。如果无法排查到原因,投标人应提供第一时间的二线专家现场支持。

2.9.2.5.安全报告记录

整合安全设备运维、网络监控分析、上线安全评估、风险分析检测、应急响应处置实战化攻防、漏洞扫描检查、安全通报处置、终端安全服务、重要时期安全保障等安全运营服务工作，形成一体化的策略、防护、检测、响应安全运营体系，强化策略管控、安全通报、漏洞管理、处置监督方面的工作机制，进一步完善边界防护、云安全防护、主机防护措施，形成实战化的安全运营计划，并落实执行。

每周汇总安全服务工作，形成《安全服务工作周报》，并提交给用户;每月汇总采购方网络安全状况，编制《网络安全月报》，并提交给用户。

年底应根据日常安全监测工作情况，对采购方网络安全总体态势进行分析，提出建设性的安全建议，编写《年度安全服务工作总结》，并提交给用户。

交付成果:《安全服务工作周报》、《网络安全月报》、《年度安全服务工作总结报告》《网络异常处置记录》《威胁监测报告》《安全策略变更记录单》《安全设备巡检表》

服务频次：服务期内按需。

2.9.3.终端安全运维

投标人需提供顽固病毒查杀、病毒威胁情报处置、接入管控、计算机补丁管理、计算机资产管理等服务。通过对终端准入、资产管理、终端管控、安全审计、移动存储管理进行以下评估让企业终端资产可知、可管、可控。

健康状况评估

评估终端当前健康状况。包括病毒查杀，漏洞扫描，防护能力开关检查，系统故障检查等。

沦陷迹象评估

评估终端的使用痕迹和入侵痕迹，IOC 查找恶意程序入侵历史和状况的查。

管控合规评估

评估终端的使用行为是否符合单位管理要求，包括违规外联，违规外设使用，违规访问行为，违规配置行为。

配置脆弱评估

评估终端的使用配置和习惯是否存在安全隐患，从身份鉴别、安全设计、访问控制、资源控制和入侵防范 5 个领域进行脆弱评估。

交付成果：《终端安全事件处置记录》

服务频次：服务期内按需。

2.9.4.安全通报

2.9.4.1.内部安全通报

基于采购人网络安全事件的安全通告机制，提供全年的内部安全通报服务，分析确认安全监测发现的安全问题、威胁情报等信息及时通告给相应的业务系统主管单位，分析确认 0day 漏洞和高风险漏洞对网内系统以及终端的影响，及时发送通报预警通知，并协助进行安全问题处置，完成处置结果确认。

内部安全通报服务主要服务对象为采购方各处室、关联单位，如河南省教育考试命题与评价中心、各地市招办(考试中心)等。

对考试院利用网络安全监测、安全预警等设备发现的安全攻击、安全事件，驻场运维人员应第一时间通过已建立的安全通告机制通报给各处室、关联二级单位、下属单位，并协助其进行安全问题整改和处置。

2.9.4.2.外部安全通报服务

配合完成主管单位发来的安全通报的处置，对网信办、国家互联网应急中心、公安部等上级网络安全管理部门发来的安全通报进行验证分析，找到有效的解决方案，提供最新的安全漏洞、威胁(0day、

系统漏洞、网络攻击)的解决办法、安全问题描述和相应的处理意见，第一时间通告并协助单位相关处室尽快进行漏洞确认和漏洞修复工作。

对安全通报的验证方式应包括但不限于渗透测试、上机检查以及安全评估等，在验证通过后，协助相关单位进行漏洞修复。如驻场运维人员无法处置时，投标人应第一时间派遣二线技术专家现场对安全事件进行验证，给出问题结论并协助整改。

交付成果:《安全检查报告》《网络安全事件报告单》

服务频次:内部通报每周一次，外部通报服务期内按需。

2.9.5.资产管理

2.9.5.1.资产台账管理

建立并维护采购人安全设备资产台账，收集各处室上报的业务系统信息，以及上线检测中的业务系统信息，更新业务系统资产台账。资产管理服务内容包括:

考试院资产管理:根据考试院实际需求，驻场运维人员应实时收集、整理考试院相关安全设备资产，建立完善资产台账;及时了解新上线的安全设备、下线的安全设备并更新台账;每月对资产台账进行检查，审核资产台账的准确性。

下级单位资产管理:驻场运维人员应对采购方业务系统下级单位上报的系统信息进行收集、整理。每月对资产台账进行检查，审核资产台账是否准确，并根据检查结果及时更新资产台账。

2.9.5.2.资产文档整理

对采购方的网络安全相关资料(包括:安全资产清单、安全拓扑图、安全设备技术资料、安全策略)进行梳理并实时维护更新。

每季度汇总整理本项目验收文档资料，用于审核和项目验收。整理安全运维服务过程中各项服务(如日常安全运维、流量威胁分析、重要时期安全保障、攻防演习、基础安全检查、网站云监测等)的文档与数据，配合采购人整理各类方案与报告。

2.9.5.3.资产维护服务

根据采购方实际业务需求和安全运维工作要求，应提供全年的终端资产统计、安全产品部署协助、安全设备迁移服务、上报数据统计等安全管理方面服务，同时提供网络安全技术支持服务。

其中，终端资产统计服务范围为:考试院本部、关联单位(包括但不限于各地市招办考试中心等);服务内容是对终端资产进行详细统计，至少应包括部门、资产类型、IP 地址、操作系统、运行情况等。

安全产品部署协助是应对采购方新上线的安全设备协助实施人员进行设备的部署。

安全设备迁移服务是应对采购方在安全设备进行迁移时，提供迁移协助。

上报数据统计是应负责对采购方、二级单位上报的数据进行统计。

交付成果:《管理支持服务记录》《安全拓扑图》、《安全设备技术资料》、《安全策略表》《安全设备资产台账》、《考试院业务系统资产台账》

服务频次:服务期内按需。

2.10.专项安全治理服务

2.10.1.数据泄露排查

数据泄露排查专项服务主要包含季度敏感信息泄露情报排查、非公开网络(暗网)数据外泄年度监控两部分。

每季度或根据实际安全需求，监控采购方的敏感信息泄露情况的情报服务，监控范围覆盖互联网的各种信息泄露渠道,全网情况一网打尽,覆盖互联网各类公开应用(如电子邮件、搜索引擎、代码托管平台、网盘等)。以攻击者视角，对收集的敏感信息进行综合分析、形成综合情报，并给出利用思路和可能的攻击链。

非公开网络(暗网)数据外泄年度监控工作以一年为周期，依托自动化的监控平台，聚焦个人信息及生产数据，协助采购方发现非公开网络(暗网)中披露的与采购方有关的敏感数据泄露事件，第一时间通告，以便开展必要的应急处置工作，降低事件对采购方的负面影响。

2.10.2.勒索、挖矿病毒排查

随着采购方应用系统的不断增加，面临的网络攻击数量和频次也越来越多。仅依靠安全监测人员针对全部安全设备产生的告警信息进行分析研判，可能存在漏报和错报风险，以致于出现勒索、挖矿安全事件，造成严重的安全后果。针对勒索、挖矿安全事件，在采购方组织开展 1 次勒索、挖矿病毒专项安全排查，彻底消除此类安全风险。

勒索、挖矿病毒专项排查服务是从全局排查视角出发，针对采购方全部办公终端及服务器进行全面专项排查，确认是否感染相关病毒，存在对应的安全隐患。

勒索、挖矿病毒专项排查以“分析研判+上机检查”的方式开展，需做好调研准备排查实施及成果汇报工作，同时在实施期间，做好风险规避措施，与客户的沟通汇报等。

2.10.3.弱口令清查

开展弱口令清查专项服务，通过在技术、管理、运营多个层面，帮助采购方从根本上杜绝由于口令问题(包括弱口令、默认口令、泄露口令等)而产生的安全问题，减少安全漏洞。

口令安全治理服务应由驻场运维人员、二线技术团队共同完成，在对资产进行梳理和分析后，制定治理实施方案，方案不得影响业务的正常运行，建立口令检测机制和整改流程，对所有弱口令进行发现整改，对于无法整改的向用户提出其它措施规避风险。口令安全治理服务的服务内容应包括:

通过主动发现方式，发现采购方所有主机、网络设备、业务系统等存在的弱口令;

通过被动监控的方式，发现采购方网络中使用的弱口令及口令复用问题:

通过威胁情报，发现可能已经泄露的口令信息。

口令安全治理服务的服务范围应包括采购方所有系统涉及的服务器、数据库中间件、网络/安全设备、终端等。

服务器，如 windows、linux 等常见主机操作系统;

数据库&中间件，如 Mysql、Oracle、Tomcat 等常见数据库&中间件;

网络&安全设备，如路由器、交换机等:

业务系统，如 OA 系统、邮件系统、核心业务系统、应用系统等;

交付成果:《口令安全检测报告》、《勒索、挖矿病毒排查报告》、《数据外泄监控分析报告》

服务频次:服务期内每季度一次。

2.11.网络和数据安全行业监管平台服务

投标人需为采购方提供一套网络和数据安全行业监管服务平台。

平台要求：平台需在国家通用要求基础上叠加行业规范要求，以行业网络运营者资产纳管为基础，以行业安全威胁统一监管为核心，立足“多主体跨部门协同、数据融通生态角色、联防联控联治机制”，构建行业网络安全长效防控体系。

交付成果：部署一套网络和数据安全行业监管服务平台。

服务频次:服务期内完成部署。

2.12.定制开发服务

中标单位需根据采购方的需求针对现有安全设备或系统，在后期使用过程中的功能不足且无法满足采购方需求时，需对指定的设备进行对应的二次开发以满足采购方对当前系统的功能需求。

交付成果：定制开发相关系统及文件

服务频次:服务期按需提供服务。

2.13.应急响应服务

2.13.1.应急预案

基于采购方网络与信息安全事件，通过对网络安全环境、重要业务系统及信息安全管理体系进行调研，制定采购方安全事件应急预案，确保能够有效应对各类信息安全事件。

编制的应急预案应符合采购方安全事件类型，具备实际可操作性，严格按照流程编制应急预案:

调研安全现状:分析采购方网络安全及重要业务系统安全防护现状，确定可能面临的安全风险，明确下一步预案编制工作计划;

确定编制计划:依据国家及行业标准，结合采购方安全管理体系及安全现状，制定合理的网络与信息安全事件应急预案编制计划:

编制应急预案:依据国家及行业标准，结合采购方安全管理体系及安全现状，编写采购方网络与信息安全事件应急预案及信息安全事件处置方案;

应急预案审核: 采购方网络与信息安全事件应急预案编制完成后需经过客户组织的专家评审，评审后才能够正式发布，确保应急预案的有效性。

2.13.2.应急响应

基于业务系统出现重大安全事件开展专家应急响应，实施安全事件检测、安全事件抑制、安全事件根除、安全事件恢复、安全事件总结，与本地驻场人员快速形成协调联动机制，快速现场(远程)开展应急工作，增强应急技术能力，健全应急响应机制。

应急响应时间:全年 7X24 小时，在驻场人员无法解决问题时，二线专业应急技术专家接到通知后 1 小时内到场。

响应方式:远程支持或现场支持。远程支持可以采用电话、E-mail，远程加密登录等手段。当远程支持无法解决问题时，中标人需派遣专业的紧急响应服务人员在第一时间到达现场提供服务。

安全事件包括但不限于:网络入慢、拒绝服务攻击、恶意代码、大规模病毒爆发、未授权访问、主机或网络异常事件、不当应用以及其他。

服务内容包括但不限于:

网站、网页出现非法言论时的紧急处置措施;

黑客攻击时的紧急处置措施;

病毒安全紧急处置措施;

软件系统遭到破坏性攻击的紧急处置措施;

数据库安全紧急处置措施;

局域网中断紧急处置措施;

设备安全紧急处置措施等。

服务目标包括但不限于:采取紧急措施，恢复业务到正常服务状态;调查安全事件发生的原因，避免同类安全事件再次发生;在需要司法机关介入时，提供法律任何的字证据等。

交付成果:《应急响应报告》《网络安全事件应急预案》

服务频次:服务期内按需提供服务。

2.14.应急演练服务

为保障采购方重要网络与信息系统的安全稳定运行，提高系统在遇到突发事件时的可用性和业务连续性，投标人应协助采购人，组织开展 1 次应急演练，包括制定应急演练方案，参与演练，协助编制应急演练总结，以提高应急人员应急工作熟练程度提升全员安全意识。

组织开展的应急演练应根据采购方实际需求，以沙盘推演、模拟演练、实际演练等形式中的一种或多种进行开展实施。在开展应急演练时，应不影响正常业务的使用以及演练必须是可控的。应急演练应做到以下工作:

演练筹备:包括演练前沟通、演练方案、演练时间、演练场地、所需调配的各项资源、正式演练通知等:

正式演练:演练防守方实施、演练攻击方实施、演练审计、演练记录、演练录影录像等;

演练总结:评估演练结果、演练结果通报、编制演练总结报告和经验、编写演练整改方案等:

安全整改:在演练完成后，按照演练整改方案协助采购方开展安全整改工作。

交付成果:《应急演练方案》、《应急演练总结》

服务频次:服务期内一年至少 1 次。

2.15.网络安全攻防演习服务

2.15.1.服务内容

投标人在不影响采购人业务的情况下，根据黑客攻击的思维，以获取权限为目的导向，不限攻击手段，通过模拟黑客的行为，尽可能全面发现导致黑客入侵的所有途径，全面挖掘采购人可能存在的各种风险点。

2.15.2.服务要求

开展攻击服务前，由中标方组织攻击红队，攻击队不少于 3 人，所有人员应具有丰富的红队经验，参加过公安、网信等监管部门组织的攻防演练。

攻击服务过程中，投标人通过专业的审计设备对所有攻击流量进行审计，并能够对攻击过程进行可视化展示。

攻击手段包括但不限于近源攻击、社工攻击、供应链攻击、网络攻击、应用攻击、0day 攻击等。

攻防演习服务结束后，投标人对发现的问题进行归纳总结，从技术、管理、意识等纬度进行分类，介绍当前存在的问题及业内最佳实践并提供整改方案与建议。

交付成果：《采购方网络实战攻防演习总结报告》

服务频次:服务期内一年至少 1 次。

2.16.数据管理能力成熟度评估服务

投标人需为采购方提供数据管理能力成熟度评估服务，全面梳理单位数据管理现状，识别分析单位数据管理能力方面存在的问题和后续可提升的方向，提供数据管理差距分析和能力提升方案，推动单位数据治理组织、数据标准、数据质量等数据管理能力落地建设，更好的支撑单位数智化建设。

交付成果:数据管理能力评估相关文档

服务频次:服务期内一年一次。

2.17.安全培训服务

采购方信息化安全需求的不断演变，为满足信息技术与自身安全保障的安全诉求，采购方有必要对技术人员和相关管理人员进行一系列的系统化的信息安全技能和知识的培训，以满足当前信息安全形势和今后日常工作的要求，整体提升安全保障运维的工作水平。

为采购方提供网络安全意识(含钓鱼邮件测试服务)、安全攻防技术培训。通过安全意识培训普及网络安全风险意识，进一步提升采购方工作人员的网络安全意识和安全防护技能，普及网络安全知识，增强应对处置信息安全风险的能力;针对安全技术人员开展攻防技术培训，提升其基础攻防技术能力。

1)组织开展 1 次网络安全意识培训。培训内容包括但不限于：

安全意识培训内容表

培训时长	课程名称	课程内容
2-3 小时	网络安全意识培训	当前信息安全领域态劳与发展趋势 信息安全意识对个人及组织单位的重要意义 个人信息安全面临的主要威胁 主要的安全应对措施 养成良好的安全习惯

2)组织开展 1 次钓鱼邮件测试。

钓鱼邮件测试应根据采购方网络环境、邮件使用习惯和特征等构造钓鱼邮件,通过互联网向目标群体定向发送钓鱼邮件，进行钓鱼测试。基于测试结果，应分析评估内部人员信息安全意识，为后续加强信息安全培训、提升技术防护手段，提供支撑依据。

3)组织开展 1 次安全攻防技术培训。培训内容包括但不限于：

安全攻防培训内容表

培训时长	课程名称	课程内容
第 1 天	网络安全及网络协议基础知识	●网络安全攻防技术发展简介 ●网络协议的概念及总体分类

		●OSI 七层模型层次划分、定义及作用、 ●TCP/IP 模型主要作用 ●OSI 七层模型概念与 TCP/IP 模型两者之间的区别: ●HTTP 的安全缺陷及共与 HTTPS 协议主要构成及安全方面的区别。 ●网络安全攻防技术演练环境使用介绍、线上培训实操演练平台使用方法讲解与指导”
第 2 天	操作系统及数据库安全基础	●Windows、Linux 系统的账户概念与账号风险和安全策略 ●Tindows 文件系统基础知识、NTFS 权限设置与系统日志审计方法; ●Linux 文件系统的格式与安全访间与权限设置 ●实操演练 Windows、Linux 系统的账号安全配置与管理，文件系统的安全配置、管理与审计。 ●Wy5QL、SQL Server 数据库基础知识及 SQL 语法及其涉及到的安全问题 ●在数据库基本配置与应用时应注意的安全事项。 ●实操演练 MySQL、SQL Server 数据库的基本安全配置、安全应用
第 3 天	安全工具基础	●Kali 操作系统、Kali 系统中的主要网络安全攻防工具的用途; ●Burp suite 工具的使用方法及主要功能(抓包、改包、爆破); ●Sqlmap 工具的基本命令使用、展示 Sqlmap 进行绕过 WAF 脚本的方法; ●Scanline、AWVs、Metasploit.Nmap 等工具的使用方法，展示利用 Nmap 扫描端口绕过防火墙的过程。 ●实操演练各个主要工具的部署、配置、用方法与技巧。
第 4 天	Web 安全基础(一)	●SQL 注入原理及基本实现方法:盲注方法堆叠注入

		方法、二次注入等方法; ●XSS 跨站脚本攻击原理及基本实现方法、存储式 XSS、反射式 XSS、DOM 式 XSS 等 Web 安全方面的基础知识; ●实操演练利用以上漏洞的主要验证及攻击实现方法。
第 5 天	Web 安全基础(二)	●常见敏感信息泄露的途径 ●常见安全配置错误 ●文件上传漏洞利用 ●文件包含漏洞利用 ●命令执行和代码执行漏洞利用 ●实操演练以上常见安全漏洞的主要验证及实现方法。

交付成果:《安全培训计划表》、《安全培训课件》

服务频次:服务期内一年至少 1 次。

3.项目服务要求

注：本项目需求的加“★”项为不可负偏离项。本项目不接受前期调研。

3.1.服务期限

本项目服务期为自合同签订之日起 36 个月

3.2.服务地点

河南省教育考试院指定地点

3.3.服务能力要求

3.3.1.项目质量要求

在项目实施全过程中，采购方有对工程质量进行监督控制的职责和权利，投标人也应按照项目管理要求进行严格的质量控制，并根据需要制定详细合理的沟通计划，应确保采购方和投标人双方能及时了解所需的信息。具体要求如下：

投标人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采购方对质量的要求。

投标人应根据项目的工作计划，对阶段性项目工作成果进行审核，并向采购方提交工作成果。通过保证各阶段性成果的质量，最终保证整个项目的质量。

所有提交给采购方的所利用工具提交的技术报告及相关资料的最后文本及工具本身均属于采购方的财产，投标人在提交给采购方之前应将上述资料进行整理归类和编制索引。

未经采购方的书面同意，投标人不得将上述资料用于与本服务项目之外的任何项目。

3.3.2.其它要求

★驻场服务人员指中标方根据合同约定派驻到采购方指定现场，专职承担相关驻场任务的项目人员。在驻场工作期间，中标方不得安排驻场人员承担其他工作任务。(**提供承诺书并加盖公章**)

★投标时提交项目成员名单，明确项目经理、全部驻场人员、主要后台技术人员，且中标后未经采购方同意不得更换。(**提供承诺书并加盖公章**)

★投标人驻场人员提供 5x8 小时驻场安全服务（特殊时期需按采购方要求进行调整),应急响应团队提供 7x24 小时应急处置服务。(**提供承诺书并加盖公章**)

★投标人应严格执行保密的有关规定，未经采购人书面同意，不得将本项目所有信息、资料向任何第三方披露、泄露。(**提供承诺书并加盖公章**)

投标人保质保量完成合同约定安全服务内容，及时反馈网络安全事件，严禁瞒报、不报、少报的情况发生。

其它满足本次招标要求的承诺。

3.4.交付时间要求

项目服务需求中 2.1.4、2.11 为合同签定完成后 15 天内交付完成，2.12 根据实际需求交付，其它需求交付时间为每项服务完成或重大事件、业务、活动完成后一周内交付。

3.5.服务考核表

为了规范中标人的安全服务，针对本项目将实行月度、年度考核机制，考核内容和考核办法详见下表。

1、总体说明：

评分表分综合考评扣分和事件考评两部分；

综合考评分采用月度打分考核，事件考评则直接对问题事件实施扣款惩戒。

2、综合考评：

综合月度考核每月考评一次，采用累计扣分法。付款考评=100-∑每月扣分值+∑每月加分值。

3、事件考评：

指定类型的事件一旦发生则直接从剩余调节基金中扣除相应数额的款项。

4、★当指标均达到 90 分（含）以上，合作伙伴获得全部调节基金；75 分以下调节基金全部扣除，75 分-90 分之间线性计算获得的调节基金，具体结算周期依照合同执行。本维保项目全年调节基金占合同总金额的 20%。

安全服务考核表

考评元素一级	考评元素二级	指标说明	打分标准	扣分	备注
综合考评					
维保能力考核	故障处理及时性	对于系统故障的响应是否及时，最终解决是否及时	每次维护需求响应时间超时，扣 2 分；每次故障解决时间超时，扣 3-5 分		
	日常维护及时性	对于技术支持、问题处理等各类日常维护工作需求的响应是否及时，最终解决是否及时	每次需求响应超时，扣 2 分；每次需求完成超时，扣 3-5 分		
	备品备件支持	乙方提供的备品备件是否充足，	每次备品备件到场不及时扣 3-5 分，备件库检查不合格，扣 5-8 分；		
	服务支持界面	建立有效的服务支持（24 小时热线，web 方式或 email 方式的沟通渠道等）；	每次服务支持未达到约定的要求，扣 3-5 分		
	产品可靠性	产品发生故障的频次	**由于系统软硬件自身引起的宕机，每次扣 5-10 分**		
	协调能力	主动协调其他相关资源（如：厂商、二线支撑人员、高级专家等）	每次不合格扣 2-4 分		

	技术培训	提供相关操作说明书、系统技术文件料等资料并有助于我方维护；提供有效的培训并达到良好的培训效果	每次操作说明和培训文档不完整，扣 2 分；每次培训效果不满足我方要求，扣 2 分		
服务规范考核	服务态度	服务态度良好，及时响应和有效解决，提交的服务报告规范有效	每次不合格扣 2-4 分		
	服务规范性	维保人员是否严格遵守我方相关规定（进出机房、维护操作）	每次不合格扣 2-4 分		
人员组织考核	人力资源投入	人员投入数量，核心人员流失	未符合合同规定的人员数量投入，每月扣 1-3 分；核心人员每流失一人，每次扣 5 分,一般事件中直接扣款补充		
	人员能力	现场维护工程师的技术能力和水平	人员能力不符合要求，每月扣 3-5 分		
	人员岗位变动	员工入职/员工离职时，《岗位变动申请表》未能在三个工作日内提交。	每发生一次扣款 2 分		

加分项	合理化加分	服务商主动进行专题优化，在提高维护效率和维护质量上取得较好成效，或提出的创新、专利工作获客户认可。	优化工作成效明显加 2 分；专利或创新成果客户通过加 5 分；双奖通过加 10 分。		
扣分合计					
事件考评部分					
关键要素一级	**关键要素二级**	**指标说明**	**扣款说明**	**扣款**	**备注**
一般事件	工作差错	工作操作不符合规范性要求，或质量不合格	按差错类型，每发生一次扣款 1000 元至 10000 元。		
	人力资源	人员投入数量，核心人员流失，人员水平不合格	未符合合同规定的人员数量投入，每月直接扣款 1000-5000；核心人员每流失一人，每次直接扣款 2000-5000,一般事件中直接扣款补充；人员能力不符合要求，每月直接扣款扣 1000-5000		
	产品质量	**由于系统软硬件自身引起的宕机**	**每发生一次，扣设备平均年维保费用的 2%-5%**		
重大事件	灰色及蓝色故障	维保人员误操作、设备故障、产品缺陷、巡检不及时等原因引起的灰色、蓝色故障等	**每发生一次扣月度调节基金的 20%-50%**		

	黄色故障	维保人员误操作、设备故障、产品缺陷、巡检不及时等原因引起的黄色故障等	**每发生一次扣月度调节基金的 50%-100%**		
	橙色及以上故障	维保人员误操作、设备故障、产品缺陷、巡检不及时等原因引起的橙色及以上故障等	**每发生一次扣月度调节基金的 100%-300%**		
	安全事件	由维保人员引起的信息安全事件（如泄露用户资料/用户系统数据/为他人提供便利给自己或他人牟取不正当利益等）；由于维保人员在机房工作引起的安全事件（如窃盗、火灾、破坏监控或门禁系统等）	**每发生一次扣月度调节基金的 100%-300%**		
扣款合计					

3.6.项目服务工具要求

随着目前网络安全态势的多元化复杂化，目前采购方现有的服务工具不能够支撑现有网络安全运行维护工作，需要投标人自带针对目前网络的流量威胁检测和漏洞扫描等工具来保障采购方的网络安全稳定运行。

★注：下表《安全服务工具表》所述设备及工具（包含但不限于）为中标方现场保障使用，采购方不予采购。所需设备由中标方按采购方需要无偿提供使用，所有工具需提前测试验收，满足需求后方可上线。同时为了保密，凡是存储过采购方数据的工具在服务期满后资产归服务采购方，不接受开源工具，所有工具不得将采集、处理的数据发送、拷贝等手段离开采购方网络。

★本项目所有工具均为正版，每类工具均为该行业头部厂商品牌，采购方不承担由于版权问题带来的任何法律责任。

《安全服务工具表》

序号	具类别	数量	是否购买	要求
1	漏洞扫描工具	1 台	否	不限 IP 数量,不限使用时间的国产扫描工具（非软件）
2	WEB 漏洞扫描工具	1 套	否	不限 IP 数量,不限使用时间专业的针对 WEB 程序存在的漏洞漏洞扫描工具（非软件）
3	流量与性能监测工具	1 套	否	不限 IP 数量,不限使用时间能够监控设备流量、性能等工具。
4	数据库漏洞扫描工具	1 套	否	不限 IP 数量，不限使用时间，不限数据库种类专业针对数据库漏洞进扫描的工具。
5	源代码安全检测工具	1 套	否	不限 IP 数量，不限使用时间,专业的源代码审计工具
6	安全态势感知平台	1 套	否	能够支持国内主流安全厂家的设备接入,平台不限 IP 数量,不限使用时间,万兆及以上分析能力，（至少包括 1 台分析平台、1 台流量探针、1 台日志审计)支持多链路接入,用于监测各个专业网络核心流量，收集多元、异构的海量日志，利用关联分析、流量分析、威胁情报等技术，持续监测网络安全态势，形成安全闭环管理，为运营人员提供威胁发现、调查发现及响应处置的安全运营工具，为安全管理者提供风险评估和应急响应的决策支撑

7	网站监测系统	1 套	否	不限 IP 和域名数量，不限使用时间，专业的网站云监测平台，可以对网站进行远程漏洞、黑链、敏感数据进行监测。
8	攻防培训平台	1 套	否	不限用户数量，不限使用时间，投标人需提供 1 套云端攻防培训平台，为采购人进行安全人员培训和学习提供服务，培训平台功能应包括但不限于：学员管理、课程管理、攻防课件管理、学习进度监测、试题、演练环境等。
9	威胁情报平台	1 套	否	投标人需提供 1 套能够提供本地化和云端化、全方位的威胁情报能力，包括及时发现关键威胁、对已有报警进行误报或分级、为事件响应提供决策需要的上下文、提供安全预警能力、提供自有情报运营能力等，为用户建设安全运营中心提供平台支撑。
10	网管系统	1 套	否	能够监控国内主流安全厂家的安全设备流量、且不限 IP、不限使用时间、不限代理数量。
11	安全管理服务器	1 台	否	最小配置要求： 2C40 核，256G 内存，10T 磁盘。

12	网络安全等级保护综合服务平台	1 套	否	平台定位于网络安全等级保护工作全阶段全过程管理，覆盖了信息系统定级、备案、等级测评、安全建设整改等工作环节，通过平台可全面梳理等保工作各项内容，描摹系统安全画像，推进等级测评、安全建设整改、监测预警、应急响应等事项落实。
13	网络和数据安全行业监管平台	1 套	否	平台需在国家通用要求基础上叠加行业规范要求，以行业网络运营者资产纳管为基础，以行业安全威胁统一监管为核心，立足“多主体跨部门协同、数据融通生态角色、联防联控联治机制”，构建行业网络安全长效防控体系。

第六章 响应文件格式

一、封面

_____（项目名称）

响 应 文 件

供应商：_____（企业电子签章或公章）

法定代表人或其委托代理人：_____（个人电子签章或签字）

年 月 日

二、评审资料

1、供应商编制响应文件时，涉及营业执照、资质、业绩、获奖、人员、财务、社保、纳税、各类证书等内容，必须在市场主体信息库中已登记的信息中选取。提供的具体内容及要求按磋商文件相应评审因素提供。

2、供应商利用投标文件制作工具制作响应文件时，评审资料部分是从主体信息库相应菜单中已录入内容进行挑选，之后形成信息表，同时获取对应扫描件进行展示。

3、以上格式如与交易平台、投标文件制作系统不一致，以平台与系统格式为准。

三、报价一览表

报价一览表

供应商名称	
报价（大写）	
报价（小写）	
服务期	
保证金	0 元
有效期	
其他声明	

备注：本表如与系统内表格格式不一致，以系统内表格为准。

四、中小微企业声明函（工程、服务）

（属于中小微企业的填写，不属于的无需填写此项内容）

本公司（联合体）郑重声明，根据《政府采购促进中小微企业发展暂行办法》（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，工程的施工单位全部为符合政策要求的中小企业（或者：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）；承建（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）；承建（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，不属于大型企业的分支机构，不存在控股股东为大型企业的情形，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（企业电子签章或公章）：

日期：

注：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成立企业可不填报。

2. 中小企业是指中华人民共和国境内依法设立,依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业的划分标准的个体工商户，在政府采购活动中视同中小企业。

3. 中小企业参加政府采购活动，应当出具本《中小企业声明函》，否则不得享受相关中小企业扶持政策。

4.中标、成交供应商享受本办法规定的中小企业扶持政策的，采购人、采购代理机构应当随中标、成交结果公开中标、成交供应商的《中小企业声明函》。

五、其他内容

1、磋商声明

致：（采购人名称）

我们收到了项目编号为_____的（项目名称）采购文件，经详细研究，我们决定参加该项目的投标活动并按要求提交响应文件。我们郑重声明以下诸点并负法律责任:

(1) 愿按照采购文件中规定的条款和要求，提供完成采购文件规定的全部工作，磋商总报价为（大写）_____元人民币（RMB￥：_____元）。

(2) 如果我们的响应文件被接受，我们将履行采购文件中规定的各项要求。

(3) 我们同意本采购文件中有关磋商有效期的规定。如果中标，有效期延长至合同终止日止。

(4) 我们愿提供采购文件中要求的所有文件资料。

(5) 我们已经详细审核了全部采购文件，如有需要澄清的问题，我们同意按采购文件规定的时间向采购人提出。逾期不提，我公司同意放弃对这方面有不明及误解的权利。

(6) 我们承诺，与采购人聘请的为此项目提供咨询服务及任何附属机构均无关联，非采购人的附属机构。

(7) 如我方中标，我方愿意按采购文件规定，向采购代理机构交纳招标代理服务费。

(8) 我公司同意提供按照采购人可能要求的与其投标有关的一切数据或资料，完全理解采购人不一定接受最低价的投标或收到的任何投标。

(9) 我们愿按《中华人民共和国民法典》履行自己的全部责任。

供应商：_____（企业电子签章或公章）

法定代表人或其委托代理人：_____（个人电子签章或签字）

地址：_____

网址：_____

电话：_____

电子信箱：_____

邮政编码：_____

年 月 日

2、报价表

供应商名称	
投标报价（大写）	
投标报价（小写）	
服务期限	
合同履行期限	
服务地点	
质量要求	
投标保证金	0 元
权利义务	符合第四章“合同条款及格式”中的实质性要求和条件。
投标有效期	
其他声明	

供应商（企业电子签章或公章）：

法定代表人或其授权的代理人（个人电子签章或签字）：

_____年_____月_____日

3、法定代表人身份证明或附有法定代表人身份证明的授权委托书

（一）法定代表人身份证明

供应商名称：_____

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_____（供应商名称）的法定代表人。

特此证明。

供应商（企业电子签章或公章）：

_____年_____月_____日

（二）授权委托书

本人_____（姓名）系_____（供应商名称）的法定代表人，现委托_____（姓名）为我方代理人。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）响应文件、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。

代理人无转委托权。

附：法定代表人身份证明和委托代理人身份证明

供应商（企业电子签章或公章）：

法定代表人（个人电子签章或签字）：

身份证号码：_____

委托代理人（个人电子签章或签字）：

身份证号码：_____

_____年_____月_____日

4、费用报价及组成分析和说明

（格式不做统一规定，由供应商自行设计）

供应商（企业电子签章或公章）：

法定代表人或其授权委托人（个人电子签章或签字）：

日期： 年 月 日

5、投标承诺函

我方（供应商名称）参加（项目名称）项目（项目编号：）的投标，根据采购文件所规定的权利和义务，在此我方承诺如下：

一、除不可抗力外，我单位如果发生以下行为，将在行为发生的 10 个工作日内，向贵方（或采购人）支付本磋商文件公布的预算金额（或最高限价）的 2%作为违约赔偿金。

1、自响应截止时间至本项目发布成交公告为止，撤销响应文件；

2、中标后不依法与采购人签订合同；

3、中标后不按照本采购文件规定向采购人提交履约保函或保证金（如有）；

4、中标后不按照本采购文件规定向贵方缴纳招标代理费。

二、我单位知晓上述行为的法律后果，承认本承诺书作为贵方（或采购人）要求我单位履行违约赔偿义务的依据作用。

供应商（企业电子签章或公章）：

法定代表人或其授权委托人（个人电子签章或签字）：

日期： 年 月 日

6、中小微企业声明函（工程、服务）

（属于中小微企业的填写，不属于的无需填写此项内容）

本公司（联合体）郑重声明，根据《政府采购促进中小微企业发展暂行办法》（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，工程的施工单位全部为符合政策要求的中小企业（或者：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）；承建（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）；承建（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，不属于大型企业的分支机构，不存在控股股东为大型企业的情形，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（企业电子签章或公章）：

日期：

注：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成立企业可不填报。

2. 中小企业是指中华人民共和国境内依法设立,依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业的划分标准的个体工商户，在政府采购活动中视同中小企业。

3. 中小企业参加政府采购活动，应当出具本《中小企业声明函》，否则不得享受相关中小企业扶持政策。

4.中标、成交供应商享受本办法规定的中小企业扶持政策的，采购人、采购代理机构应当随中标、成交结果公开中标、成交供应商的《中小企业声明函》。

7、监狱企业证明材料（如有）

由供应商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

8、残疾人福利性单位声明函（如有）

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。

供应商名称（公章）：

日　期：

9、商务条款偏离表

序号	内容	标书要求	投标响应	是否偏离	备注
1	采购内容				
2	质量要求				
3	服务期限				
4	服务地点				
5	合同履行期限				
6	投标有效期				
7	投标承诺函				
…	…				
	其他商务条款				

备注：1、供应商将任何不同于竞争性磋商文件的商务条款列于“偏离表”中，同时在“偏离表”中注明其他条款无偏离；

2、若所有条款均无偏离也应在“偏离表”中注明所有条款均无偏离

供应商（企业电子签章或公章）：

法定代表人或其授权的代理人（个人电子签章或签字）：

_____年_____月_____日

10、供应商资格审查资料

（1）具有独立承担民事责任的能力（提供有效的企业法人营业执照副本或法人证书或其他组织、自然人的有效证照）；

（2）供应商应具有公安部第三研究所颁发的有效的《网络安全等级测评与检测评估机构服务认证证书》（提供证书）；

（3）具有良好的商业信誉和健全的财务会计制度（提供完整的 2023 年度或 2024 年度经审计的财务报告或银行出具的资信证明）；

（4）有依法缴纳税收和社会保障资金的良好记录(提供近六个月内任意 1 个月的纳税及社保缴纳证明，如依法免税或纳税零申报须提供相关证明材料）；

（5）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名单、重大税收违法失信主体名单、政府采购严重违法失信行为记录名单的供应商，拒绝参与本项目政府采购活动。[查询渠道:“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）]；

（6）具有履行合同所必需的设备和专业技术能力（提供声明）；

（7）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（提供声明）。

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

声明

致：_____（采购人名称）

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，具有履行合同所必需的设备和专业技术能力，具有良好的商业信誉和健全的财务会计制度，并具有提供本次招标服务的能力。

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

若上述内容不属实，我公司愿取消本项目投标资格，并将承担相关法律责任，接受处理。

特此声明。

供应商（企业电子签章或公章）：

法定代表人或其委托代理人（个人电子签章或签字）：

日期： 年 月 日

11、业绩清单

序号	项目名称	项目单位	合同金额	合同签订时间	完成时间	联系人	联系电话

说明：在上表中列出近年以来的类似项目业绩清单，同时附相关证明材料。

12、拟投入项目人员情况

序号	姓名	性别	年龄	学历	证书名称及级别	在项目中的岗位	备注

注：本表后附项目相关人员证书、社保证明等相关证明材料。

13、项目需求偏差表

序号	需求名称和条款号	项目要求		对竞争性磋商文件偏差	描述	备注
		招标书	投标书			
1						
2						
	……					

注：供应商应对竞争性磋商文件中的项目需求逐项做出响应，在“项目需求偏差表中”列明项目需求要求、投标响应情况，并标明偏差情况。

供应商（企业电子签章或公章）：

法定代表人或其委托代理人（个人电子签章或签字）：

日期： 年 月 日

14、项目服务方案

15、供应商认为需要加以说明的其他内容