INTERNATIONAL
TRADE & TENDERS
国贸招标

竞争性磋商文件

项目名称：2026 年度河南省福利彩票发行中心（河南省养老事业发展中心）信息安全服务
项目编号：豫财磋商采购-2026-125
采 购 人：河南省福利彩票发行中心（河南省养老事业发展中心）
采购代理机构：河南省国贸招标有限公司

2026 年 7 月

特 别 提 示

一、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-办事指南-《CA数字证书办理指南》）；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-办事指南-《河南省公共资源电子交易平台市场主体信息库登记指南（工程建设、政府采购》）；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，按网上提示报名并下载采购文件及资料（详见https://hnsggzyjy.henan.gov.cn/公共服务-办事指南）。

二、响应文件制作

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（办事指南及下载专区）：下载“响应文件制作工具安装包压缩文件下载”等。

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)的采购文件。

3、供应商须在响应文件递交截止时间前制作并提交：加密的电子响应文件（*.hntf 格式）,应在响应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；

4、加密的电子响应文件为“河南省公共资源交易中心（https://hnsggzyjy.henan.gov.cn/）”网站提供的“响应文件制作工具”软件制作生成的加密版响应文件。

5、供应商在制作电子响应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）。

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,登录远程开标大厅（http://hnsggzyjy.henan.gov.cn/）,在线准时参加开标活动并进行文件解密、答疑澄清等（详见http://https://hnsggzyjy.henan.gov.cn/公共服务-办事指南-河南省公共资源电子交易平台不见面服务系统使用指南）。开标时供应商应登录河南省公共资源电子交易平台不见面服务系统，使用CA数字证书在规定时间远程解密，未在规定时间内解密的响应文件将被拒绝。

7、供应商编制响应文件时，提供的具体内容及要求按采购文件相应评审因素提供。

8、采购文件格式所要求包含的全部资料应全部制作在响应文件内，严格按照本项目采购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，否则将存在响应文件被拒绝的风险。开标一览表（投标函），须严格按照格式编辑，并作为电子开评标系统上传的依据。

9、响应文件以外的任何资料招标人和招标代理机构将拒收。

10、供应商编辑电子响应文件时，根据采购文件要求用法人CA密钥和企业CA密钥进行签章制作；最后一步生成电子响应文件（*.hntf格式和*.nhntf格式）时，只能用本单位的企业CA密钥。

11、未尽事宜请供应商仔细阅读河南省公共资源电子交易平台相关操作手册或说明。。

三、澄清与变更

采购人、采购代理机构对已发出的采购文件进行的澄清、更正或更改，澄清、更正或更改的内容将作为采购文件的组成部分。采购代理机构将通过网站“变更公告”和系统内部“答疑文件”告知供应商，对于各项目中已经成功报名并下载采购文件的项目供应商，系统将通过第三方短信群发方式提醒供应商进行查询。各供应商须重新下载最新的采购文件和答疑文件，以此编制响应文件。供应商注册时所留手机联系方式要保持畅通，因联系方式变更而未及时更新系统内联系方式的，将会造成收不到短信。此短信仅系友情提示，并不具有任何约束性和必要性，采购代理机构不承担供应商未收到短信而引起的一切后果和法律责任。

四、注意事项

因河南省公共资源交易中心平台在开标前具有保密性，供应商在响应文件上传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负。

在项目开启后，竞争性磋商小组对供应商发起的澄清、磋商以及最后报价等事项均通过系统进行，供应商应密切关注系统通知、提示的待办事项，并按照系统要求进行相应回复及报价，否则，由此引起的所

有后果和责任由供应商承担。采购代理机构不承担一切后果和法律责任。

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

2026年度河南省福利彩票发行中心（河南省养老事业发展中心）信息安全服务项目竞争性磋商公告

项目概况

2026年度河南省福利彩票发行中心（河南省养老事业发展中心）信息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（https://hnsggzyjy.henan.gov.cn/）”网上，凭企业CA数字证书进行网上获取竞争性磋商文件，并于2026年8月3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-2026-125

2、项目名称：2026年度河南省福利彩票发行中心（河南省养老事业发展中心）信息安全服务

3、采购方式：竞争性磋商

4、预算金额：190万元

最高限价：190万元

序号	包号	包名称	包预算（元）	是否专门面向中小企业	包最高限价（元）
1	豫政采豫政采(2)20261176	2026年度河南省福利彩票发行中心(河南省养老事业发展中心)信息安全服务	1900000.00	是	1900000.00

5、采购需求

（1）服务范围：提供信息安全服务（包括必要的软硬件工具配套），涵盖河南省福利彩票发行中心(河南省养老事业发展中心)生产一机房、生产二机房、数据管理中心三个机房和生产系统（含电脑票热线销售系统和即开票销售系统）、计算机辅助管理系统（CAM）（含运营管理信息系统（OMIS）、办公自动化（OA）和渠道营销管理平台）、门户网站系统（河南福彩网）三个系统，并且具有可扩展性。

（2）服务要求：首先对河南福彩信息中心网络和应用进行安全域划分，将业务外网和生产内网分开，并进一步细化为外部办公区、外部业务区、内部服务区和核心业务区等，并根据不同的业务类型制定不同的安全建设方案。另外，对现有安全体系和安全策略进行优化和调整，并根据按照《信息系统安全等级保护测评要求》（GB/T22239-2019）等政策文件的新要求补充新的安全措施和安全防护手段。

（3）服务期限：不少于365天，具体服务周期以总预算除以单日服务费报价后取整位数确定。

（4）服务地点：河南省福利彩票发行中心(河南省养老事业发展中心)指定点（包括但不限于省中心机房及全省各地市销售网点）

（5）质量要求：达到国家及行业合格标准和采购要求。

6、合同履行期限：同服务期限。

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：是

二、供应商资格条件

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：本项目专门面向中小企业采购。中小企业划分标准所属行业：软件和信息技术服务业。

3、本项目的特定资格要求

（1）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、重大税收违法失信主体、政府采购严重违法失信行为信息记录名单的供应商，拒绝参与本项目的磋商；【查询渠道：“信用中国”网站（https://www.creditchina.gov.cn/）、中国政府采购网（http://www.ccgp.gov.cn/）】。

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

4、本次不接受联合体。

三、采购文件的获取

1、时间：2026 年 7 月 22 日至 2026 年 7 月 28 日，每天 00:00 至 12:00，12:00 至 23:59（北京时间）

2、地点：河南省公共资源交易中心网站下载

3、方式：网上获取。市场主体需要完成 CA 数字证书办理，凭 CA 密钥登陆河南省公共资源交易中心系统并在规定时间内按网上提示下载采购文件，获取采购文件后，供应商请到河南省公共资源交易中心网站下载最新版本的投标响应文件制作工具安装包，并使用安装后的最新版本投标响应文件制作工具制作电子投标响应文件。

4、售价：0 元。

四、响应文件提交截止时间地点

1、时间：2026 年 8 月 3 日 9 时 00 分（北京时间）

2、地点：加密电子响应文件须在响应文件提交截止时间前通过“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，加密电子投标响应文件逾期或未按规定提交/上传的，采购人不予受理。

五、响应文件的开启时间及地点

1、时间：2026 年 8 月 3 日 9 时 00 分（北京时间）

2、地点：河南省公共资源交易中心网站首页“不见面开标大厅”，注意事项：（1）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。（2）供应商未在规定时间解密的，其投标响应文件采购人将拒绝接收。

六、发布公告的媒介及公告期限

本次公告在《河南省政府采购网》、《河南省公共资源交易中心网》上发布。公告期限 3 个工作日。

七、其他补充事宜

本项目执行优先采购节能环保、环境标志性产品、优先采购自主创新产品，扶持不发达地区和少数民族地区，促进中小企业、监狱企业、残疾人福利性企业发展等政策。

八、联系方式

1、采购人信息

名称：河南省福利彩票发行中心（河南省养老事业发展中心）

地址：郑州市晨旭路 8 号

联系人：马先生　　联系方式：0371-65507927

2、采购代理机构

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：倪涛 全乐 肖鹏　　联系方式：0371-69131983

3、项目联系方式

项目联系人：倪涛

联系方式：0371-69131983

第二章　供应商须知

供应商须知前附表

条款号	内容	说明与要求
2.1	采购人	名称：河南省福利彩票发行中心（河南省养老事业发展中心） 地址：郑州市晨旭路 8 号 联系人：马先生　　联系方式：0371-65507927
2.2	代理机构	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：倪涛 全乐 肖鹏　　联系方式：0371-69131983
3.1	项目名称	2026 年度河南省福利彩票发行中心（河南省养老事业发展中心）信息安全服务
3.2	项目编号	豫财磋商采购-2026-125
3.3	标包划分	本项目不划分标段。
3.4	资金来源	财政资金
3.5	服务范围	见第一章 竞争性磋商公告 一
3.6	服务期限	见第一章 竞争性磋商公告 一
3.7	服务地点	见第一章 竞争性磋商公告 一
3.8	质量要求	见第一章 竞争性磋商公告 一
3.9	公告发布媒介	见第一章 竞争性磋商公告 六
3.10	现场考察及答疑会	本项目不组织
4.1	合格供应商资格条件	见第一章 竞争性磋商公告 二、供应商资格条件
10.1	文件语言	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。
12.1	市场主体信息库	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，应根据河南省公共资源交易中心的相关规定进行备案、使用，具体详见河南省公共资源交易中心相关通知。 2） 因入库信息不合法、不真实、不清晰、不准确、不完整、无效、错误或信息处于编辑中、待验证状态等对交易活动所造成的一切后果，由供应商自行负责。
13.1	报价	本次总报价须为人民币报价，包含：本项目实施完成价（包括：维护和维保服务所需的设备、材料、人员、相关服务费、税费和相关费用等完成此项目的所有费用）。对在合同实施过程中可能发生的其它费用（如：增加耗材、材料涨价、人工、运输成本增加等因素），采购人概不负责。对于本文件未列明，而供应商认为必需的费用也需列入总报价。在合同实施时，采购人将不予支付供应商没有列入的项目费用，并认为此项目的费用已包括在总报价中。 注：供应商报价应按照单日服务费报价。所报价格计算保留小数点后两位，四舍五入。 由于电子交易平台的报价模板受限制的特殊性，供应商为了说明总价，可在首次报价备注或在最后报价附件提交说明。说明的内容可为单日报价乘以服务期得出总价。

条款号	内容	说明与要求
		多轮次报价 响应性文件中报价为首轮次报价，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。供应商应当对竞争性磋商的最后报价在电子交易平台规定的时限内（一般为30分钟，具体按现场规定时间为准）上传递交给竞争性磋商小组，竞争性磋商报价以供应商的最后报价为准。 由于电子交易平台的报价模板受限制的特殊性，供应商为了说明总价，可在首次报价备注或在最后报价附件提交说明。说明的内容可为单日报价乘以服务期得出总价。（说明总价属于自愿说明，因未说明所产生的所有责任与结果，均由供应商自行承担）。 分项价格的价格按（首次报价－最后报价)除以首次报价后得出的优惠率视同分项价格的优惠浮动值(特定分项价格除外)。此优惠率调整原则适用于合同内价格的计算及项目增减、变更时价格的计算。 提交最后报价的供应商不得少于3家。 注：根据财库〔2015〕124 号文规定，采用竞争性磋商采购方式采购的政府购买服务项目，在采购过程中符合要求的供应商只有 2 家的，竞争性磋商采购活动可以继续进行；若在此状态下，成交候选供应商推荐 2 名。（本项目不适用）
13.2	备选方案	不接受
13.4	采购预算	190 万元
15.1	磋商响应有效期	60 天。（指：响应文件递交开启截止之日起）

条款号	内容	说明与要求
16.1	供应商资格的证明文件	参加本项目政府采购活动的供应商应具备政府采购法二十二条和本项目采购文件规定的条件，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按无效标处理。其中证明材料在诚信信息库中自行备案并选择、响应内容同时可在平台其它内容中上传。 1、具备独立承担民事责任的能力 附：提供有效的法人或者其他组织的营业执照等主体资格证明，自然人的身份证明的截图或复印件或扫描件（企业电子公章） 2、具有良好的商业信誉和健全的财务会计制度 附：可以选用以下三项中任一项的截图或复印件或扫描件（企业电子公章）： （1）由会计师事务所出具的 2024 年度或 2025 年度完整的财务审计报告。 （2）近 3 个月内供应商基本开户银行出具的资信证明。 （3)财政部门认可的政府采购专业担保机构出具的投标担保函的扫描件或复印件。 3、有依法缴纳税收和社会保障资金的良好记录 附：提供 2026 年度内任意 1 个月的供应商依法缴纳税收和社会保障资金的税收完税证明材料的截图或复印件或扫描件（企业电子公章） （如有依法免税或不需要缴纳社会保障金的，必须提供相应证明） 4、履行合同所必需的货物和专业技术能力的书面声明 （见第六章 竞争性磋商响应文件格式 一） 5、在经营活动中没有重大违法违规记录的书面声明 （见第六章 竞争性磋商响应文件格式 一） 6、无不良信用记录承诺 （见第六章 竞争性磋商响应文件格式 一） 7、无行政及经济关联或利害关系的承诺 （见第六章 竞争性磋商响应文件格式 一） 8、政府采购政策落实 （见第六章 竞争性磋商响应文件格式 一）中小微企业声明函、监狱企业证明材料（若有）、残疾人福利性单位声明函（若有）
18.2	磋商保证金	无
19.2	响应文件的签署及规定	供应商在制作响应文件时，应将响应格式中有明确有签字、盖章处进行签字或签章或加盖公章（上传交易平台的电子版响应文件应分别为企业电子公章、个人电子签章或签名）
19.3	响应文件的份数	加密的电子响应文件 1 份
20.1	响应文件密封、标识要求	加密的电子响应文件（*.hntf 格式）应按电子交易平台要求进行加密，在平台系统指定位置上传。供应商未按要求加密、上传所产生的所有责任与结果，均由供应商自行承担。
21.1	响应文件递交截止时间、地点	见第一章 竞争性磋商公告 四
24.1	开标（开启）时间、地点	见第一章 竞争性磋商公告 五

条款号	内容	说明与要求
25.1	磋商小组	采购人将依法组建 3 人以上单数的磋商小组，其成员从河南省政府采购专家库中随机抽取的评审专家和采购人代表共同组成，其中随机抽取的专家不少于总人数的三分之二。
30.1	履约保证金	合同签订后，于服务起始日前二十个工作日内,供应商向采购人支付合同价款 3%的履约保证金（履约保证金户名：河南省福利彩票发行中心(河南省养老事业发展中心)，账号：246801819248，开户行：中行金水支行）。待维护期满（按日历计算）后三十个工作日内，采购人向供应商一次性无息返还 3%的履约保证金。
31.3	付款条件	采购人在收到履约保证金且供应商出具合法发票后十五个工作日内，采购人向供应商支付合同总价款的 100%。发票是付款的先决条件，如供应商无提供发票，采购人有权拒绝支付合同款。
32.1.1	代理服务费收取	参照河南省招标投标协会豫招协【2023】002 号文件标准规定（以预算金额按差额定率累进法计算），由成交供应商向代理机构缴纳招标代理服务费，服务费金额 27800 元。
32.3	代理服务费缴纳账户信息	单位名称：河南省国贸招标有限公司 开户银行：中信银行郑州南阳路支行 账　　号：7392 4101 8260 0025 233 行　　号：302491039249
35	支持中小企业、监狱企业、残疾人企业发展	根据财政部 2021 年 2 月 20 日发布《政府采购促进中小企业发展政策问答》 专门面向中小企业采购的项目或者采购包，不再执行价格评审优惠的扶持政策。
36	中小企业划分标准所属行业	本项目专门面向中小企业采购。中小企业划分标准所属行业：软件和信息技术服务业。从业人员 300 人以下或营业收入 6800 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 50 万元及以上的为小型企业；从业人员 10 人以下或营业收入 50 万元以下的为微型企业。
41	信用信息查询	查询渠道：“信用中国”网站（https://www.creditchina.gov.cn/）、中国政府采购网（http://www.ccgp.gov.cn/）
42.2.1	接收质疑函的方式	供应商应在法定质疑期内以书面形式向采购人、采购代理机构提出质疑，并按要求递交质疑函原件及相关证明材料。
42.2.2	质疑相关联系事宜	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 联系电话：0371-69131983
44	其他需要说明的事项	本前附表是对供应商须知的补充及强调，如前附表与供应商须知存在不一致之处，以前附表为准。

条款号	内容	说明与要求
44	落实政府采购合同融资贷款政策	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。

一、说明

1、适用范围

1.1 本采购文件遵循《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》、《政府采购竞争性磋商采购方式管理暂行办法》（财库〔2014〕214 号）、《财政部关于政府采购竞争性磋商采购方式管理暂行办法有关问题的补充通知》（财库〔2015〕124 号）、《政府采购评审专家管理办法》（财库〔2016〕198 号）、《河南省政府采购专家管理操作规程》、《财政部关于推动解决政府采购异常低价问题的通知》（财库〔2026〕2 号）等法律法规，是本项目采购文件的规范性文件，适用于本项目涉及的采购内容、报价、商务和技术部分等方面，是编制采购文件的依据。

2、定义

2.1“采购人”供应商须知前附表中所述的、依法进行采购的企事业单位、团体组织等。

2.2“采购代理机构”系指组织本次竞争性磋商采购的社会采购代理机构。

2.3“采购方”系指“采购人”和“采购代理机构”。

2.4“供应商”系指在中国境内注册、具有提供本项目标的物的生产、采购、供应的能力、向采购代理机构购买采购文件并提交响应文件的供应商。

2.5“采购文件”系指采购机构在电子交易平台内公开发布的用于本次采购的规范性文件，文件中所述“磋商文件”、“竞争性磋商文件”与“采购文件”系指本文件。

2.6“响应文件”系指供应商在响应文件递交开启截止时间前在电子交易平台中加密上传的响应文件，文件中所述 “竞争性响应文件”与“响应文件”系指本文件。

2.7“货物”系指采购文件规定供应商为采购人提供的标的物，文件中所述 “货物”与“产品”系指货物。

2.7“服务”系指采购文件规定供应商为采购人提供采购标的物伴随的服务而应承担的相关其他类似的义务。

3、采购项目概况

3.1 项目名称：见供应商须知前附表；

3.2 项目编号：见供应商须知前附表；

3.3 标段（标包）划分及名称：见供应商须知前附表；

3.4 资金来源：见供应商须知前附表；

3.5 服务范围：见供应商须知前附表；

3.6 服务期限：见供应商须知前附表；

3.7 服务地点：见供应商须知前附表；

3.8 质量要求：见供应商须知前附表；

3.9 公告发布媒介：见供应商须知前附表；

3.10 现场考察及答疑会：见供应商须知前附表。

4、合格的供应商

4.1 合格供应商的资格条件：见供应商须知前附表。

4.2 按采购文件要求提交响应文件；

4.3 遵守供应商各项承诺、义务和纪律；

4.4 遵守招标投标相关法律等有关法律、法规，如有违反，将视为不合格供应商，其响应文件无效。

4.5 联合体投标：不接受。

4.6 采购文件中规定的其他条件。

5、费用

5.1 供应商应承担其在响应文件准备、编制、上传及合同签订的整个过程中发生的一切费用而不论最终评审结果如何。

二、采购文件说明

6、采购文件的构成

6.1 采购文件用以阐明所需货物与服务、评审程序和合同条款等内容；采购文件由下述部分组成：

第一章 竞争性磋商公告

第二章 供应商须知

第三章 评审程序、方法及标准

第四章 合同草案及主要条款

第五章 采购需求和服务要求

第六章 竞争性磋商响应文件格式

6.2 供应商应详细阅读采购文件中的所有条款内容、格式、表格和所涉及的相关规范。如果供应商不按采购文件的要求提交响应文件和资料的，或者响应文件没有对采购文件提出的实质性要求和条件做出响应，可能将导致响应文件不被接受，其后果由供应商自己负责。

6.3 供应商被视为（或有义务）充分熟悉本项目所在地的与履行合同有关的各种情况，包括自然环境、气候条件、劳动力及公用设施等，本采购文件不再对上述情况进行描述。

6.4 供应商必须详阅采购文件的所有条款、文件及表格格式。供应商若未按采购文件的要求和规范编制、提交响应文件，将有可能导致响应文件被拒绝接受。

7、采购文件的澄清

7.1 供应商对采购文件如有疑问，需要求采购方进行澄清的，但应在响应文件递交开启截止时间前在电子交易平台上进行提问，要求采购方对采购文件予以澄清。采购方将在规定时间内通过电子交易平台系统内部“答疑文件”发布，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。

8、采购文件的修改

8.1 在响应文件上传截止时间前，采购方可根据需要和（或）依据供应商要求澄清的问题而修改采购文件，并通过电子交易平台系统内部“答疑文件”发布，对于项目中已经成功获取并下载采购文件的供应商，系统将通过第三方短信群发方式提醒供应商进行查询。各供应商须重新下载最新的答疑文件，以此编制响应文件。

8.2 采购文件的修改书将构成采购文件的一部分，对供应商具有同样的约束力。

8.3 为使供应商有足够的时间按采购文件的修改要求考虑修正响应文件，采购代理机构可酌情推迟响应文件上传的截止时间和开标时间，并通过电子交易平台系统第三方短信群发方式提醒每一供应商。

8.4 澄清或者修改的内容可能影响响应文件编制的，将在首次响应文件截止时间至少 5 日前在电子交易平台系统发布并通过第三方群发短信提醒，不足 5 日的，将顺延提交首次响应文件截止时间。

三、响应文件的编写

9、要求

9.1 供应商应仔细阅读采购文件的所有内容，按采购文件的要求制作并提供响应文件；供应商应保证所提供的全部资料的真实性、准确性、有效性，并使其对采购文件的实质性要求做出完全的响应，否则，其响应文件可能被拒绝。

10、语言及计量单位

10.1 除供应商须知前附表另有规定外，采购文件、响应文件以及来往信函，在未获得采购人特别要求时，应以中文书写。

10.2 除在采购文件的另有规定外，计量单位应使用中华人民共和国法定计量单位（国际单位制和国家选定的其他计量单位）。

10.3 采购文件中所表达的时间均为北京时间。

11、响应文件的组成

11.1 供应商必须按照采购文件的要求制作并提交响应文件，证明其是合格的供应商和成交后具有履行合同的能力。

11.2 响应文件应包括商务部分（主要有资格证明、授权书、报价、商务偏离）、技术部分（含技术偏离、货物技术响应、实施方案即服务承诺）、需要提供的其它内容部分，具体内容见第六章 竞争性磋商响应文件格式，格式中若表明“如有”的，供应商可根据自身情况提交，不作为非实质性响应的判定。

11.3 供应商应的响应文件中所做的说明要有充分的解释和依据，以证明其所提供内容符合采购文件的各项要求。

12、响应文件内容填写说明

12.1 因本项目实行全过程电子化采购，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，须在主体信息库相关格式中登记体现，有利于评审选取已登记的信息为评审依据。请各供应商及时根据河南省公共资源交易中心的要求补充及完善其市场主体信息库中相应内容。

12.2 供应商应按采购文件要求的内容填写编制响应文件，有规定格式的按规定格式填写，无规定格式的由供应商自拟。

12.3 响应文件不得漏项或虚报，否则将可能导致其投标响应被拒绝。

13、报价

13.1 根据采购文件第五章采购需求和服务要求的内容，供应商应对所需采购内容进行总报价。总报价见供应商须知前附表。

13.2 供应商应充分考虑市场风险和国家政策性风险系数，根据企业具体情况在合理的范围内自主报价，但不得低于企业实际成本。报价应以人民币为结算货币，供应商只要投报了一个确定数额的总价，无论分项价格是否全部填报了相应的金额或免费字样，该报价应被视为已经包含了但并不限于各该项采购货物或服务和其相关内容的费用及所需缴纳的所有税费，合同签定后价格将不得变动。

13.3 除非供应商须知前附表另有规定，供应商应在填写报价一览表时注明全部采购内容的报价，采购方不接受有选择性报价或替代方案。

13.4 采购人不接受超出采购预算的报价，首次报价及最后报价超出预算价的均将其投标响应被拒绝，采购预算见供应商须知前附表。

14、报价货币

14.1 响应文件中所有报价的币种一律采用人民币填报。

15、磋商响应有效期

15.1 磋商响应有效期见供应商须知前附表。有效期短于这个规定期限的报价，将被拒绝；

15.2 磋商响应有效期从响应文件递交开启截止之日起开始计算。

15.3 特殊情况下，采购方可于磋商响应有效期满之前要求供应商同意延长有效期，要求与答复均应以电子交易平台通知形式。

16、供应商资格的证明文件

16.1 供应商必须按照采购文件规定提交证明其有资格及有能力履行合同的文件，作为响应文件的一部分。资格证明文件内容见供应商须知前附表。

17、技术响应文件

17.1 供应商须提交证明其服务内容符合采购文件规定的技术响应文件，作为响应文件的一部分。

17.2 技术证明文件可以是文字资料、图纸和数据，并须按采购文件第六章要求填写或提供。

18、磋商保证金

18.1 磋商保证金：见供应商须知前附表。

19、响应文件的签署及规定

19.1 组成响应文件的各项资料(本须知第 11 条中所规定)均应遵守本条。

19.2 供应商应根据采购文件第六章竞争性磋商响应文件格式的要求，填写、签署，同时按要求盖章。

19.3 响应文件提供份数：见供应商须知前附表。所有的响应文件评审时以上传系统的加密电子响应文件为准。

19.4 响应文件不得涂改和增删，如有修改错漏处，必须由法定代表人或与响应文件中授权委托书中所述的同一签署人签字或签章。

19.5 响应文件上传不清晰或因字迹潦草或表达不清所引起的后果由供应商负责。

19.6 采购方概不接受以现场递交、邮寄、电话、传真形式的响应文件。

四、响应文件的递交

20、响应文件的标记

20.1 供应商上传的加密电子响应文件（*.hntf 格式）应按照电子交易平台的要求进行加密。

21、递交响应文件的截止时间

21.1 供应商制作的响应文件必须按供应商须知前附表中规定的递交截止时间之前上传至电子交易平台指定位置。

21.2 出现第 8 款因采购文件的修改推迟截止日期时，则按采购方修改通知规定的时间递交。

21.3 因交易中心平台问题无法上传电子响应文件时，请在工作时间与公共资源交易中心联系。

22、迟交的响应文件

22.1 因电子交易平台的特殊性，未在响应文件递交开启截止时间前上传的响应文件，在递交截止时间后，将无法上传，采购方不予接受迟交的响应文件。

23、响应文件的补充、修改、撤回及撤销

23.1 在本章 21.1 项规定的响应文件递交截止时间前，供应商可以对所上传的响应文件进行补充、修改或者撤回，补充或修改的响应文件应在响应截止时间前重新制作后加密上传至电子交易平台覆盖原响应文件，响应文件撤回的应在响应文件递交开启截止时间前在电子交易平台内使用企业 CA 对已上传的响应文件进行撤回。

五、开标及评审

24、开标(开启)

24.1 采购方按采购文件规定的时间、地点及相关交易中心电子交易平台规定进行电子开标。

24.2 本次实施“远程不见面开标”，供应商不抵达开标现场，在开标过程期间进行加密的电子响应文件远程解密，因供应商原因无法解密电子响应文件，由此产生的后果由供应商自行承担；

24.3 供应商对开标结果有异议的应在规定时间内远程线上进行提问，否则，视同同意开标结果；

24.4 远程解密，具体操作流程见河南省公共资源交易中心操作指南，如在解密过程中因系统出现问题请与河南省公共资源交易中心电子交易平台统一技术服务电话：400 998 0000，咨询电话 0371-61335566 联系；

24.5 采购方按采购文件规定的时间以及相应规定在指定的地点召开评审会议，磋商小组由采购人代表及评审专家共同组成，负责对所有响应文件进行评审并推荐成交供应商候选人，供应商不参加现场评审会议。

25、磋商小组

25.1 采购方将按有关规定组建，具体组成见供应商须知前附表。

25.2 磋商小组独立开展工作，对响应文件进行审查、澄清、评估和比较，并推荐成交候选人。

25.3 磋商小组将对供应商的商业、技术秘密予以保密。

26、评审

26.1 评审原则：本次采购活动遵循公平、公正、科学和择优的原则，坚持采购文件的所有相关规定，公平开展评审。

26.2 评审程序：具体内容见第三章 评审程序、方法及标准

六、授予合同

27. 合同授予标准

27.1 采购人将把合同授予被确定为实质性响应采购文件要求并有履行合同能力且评审得分排名第一的成交候选人为成交供应商。

27.2 排名第一的成交供应商放弃履约、因不可抗力提出不能履行合同或采购人发现其响应资料有虚假不实之处，采购人可以确定排名第二的成交候选人为成交供应商。排名第二的成交候选人也出现前述情况，将顺延至第三成交候选人，采购人也可以重新开展采购活动。

28、确定成交供应商

28.1 采购人依法从磋商小组推荐的成交候选人中确定成交供应商。

28.2 合同将授予通过初步评审，且技术、商务最大程度满足项目需要且评审得分排序第一的成交候选人。

29、成交通知

29.1 采购人按规定确定成交供应商后，在指定的信息发布媒体上发布成交公告，同时向成交供应商发出《成交通知书》。

29.2《成交通知书》将作为签订合同的依据。

30、履约保证金

30.1 在签订合同前，成交供应商应按供应商须知前附表规定的形式、金额向采购人提交履约保证金。

31、签订合同

31.1 成交供应商在接到《成交通知书》后，应及时按采购人指定的时间、地点与采购人签订合同。

31.2 采购文件、成交供应商的响应文件及其评审过程中的澄清和承诺文件等，均为签订合同的依据，成交供应商不得再提出任何背离上述文件内容的条件或要求。

31.3 采购人不接受付款条件的偏离，付款条件见供应商须知前附表。

32、代理服务费

32.1 成交供应商应按以下规定向代理机构交纳代理服务费。

32.1.1 代理服务费：本项目代理服务费按照供应商须知前附表所规定的标准收取。

32.1.2 代理服务费的交纳方式：成交供应商应按规定的标准一次向采购代理机构以对公转账的形式或其它约定方式向采购代理机构缴纳代理服务费，在领取成交通知书时，同时提交领取成交通知书专项授权书及代理服务费缴纳的证明材料。

32.2 代理服务费缴纳账户信息见供应商须知前附表。

33、法律追索和赔偿

33.1 成交供应商未按上述规定向代理机构交纳足额代理服务费的，代理机构可采用法律手段追索和要求赔偿。

七、政府采购政策

34、采购进口产品。（本项目无）

35、本项目专门面向中小企业及监狱企业采购项目：见供应商须知前附表。根据财政部、工业和信息化部《政府采购促进中小企业发展管理办法》（财库[2020]46 号）、财政部《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）、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。本项目专门面向中小企业采购的项目或者采购包，不再执行价格评审优惠的扶持政策。

36、中小企业划分标准所属行业。见供应商须知前附表。相关文件详见本章附件。

37、有创新政府采购政策、绿色发展的货物。（本项目无）

38、采购节能、环境标志货物。（本项目无）

39、采购涉及信息安全的货物。（本项目无）

40、采购国家强制性的货物。（本项目无）

41、信用信息查询及使用见供应商须知前附表。根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》(财库[2016]125 号)的规定，对列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，

拒绝其参与本项目采购活动。

八、询问、质疑及投诉

42、询问和质疑

42.1 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。

42.2 质疑函的接收及回复

42.2.1 接收质疑函的方式：详见供应商须知前附表。

42.2.2 质疑函接收联系事宜:详见供应商须知前附表。

42.3 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。质疑函格式详见本章附件。

42.4 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做出答复的，可以在答复期满后 15 个工作日内按的规定向财政部门提起投诉。

42.5 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。

42.6 其它未尽事宜按《政府采购质疑和投诉办法》（财政部令第 94 号）执行。

九、其他

43、解释权：本采购文件的解释权属于采购人和采购代理机构。

44、其他：其他需要说明的事项见供应商须知前附表。

附件 1：

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。

附件 2：

投诉书范本

一、投诉相关主体基本情况

投诉人：_____

地址：_____ 邮编：_____

法定代表人/主要负责人：_____

联系电话：_____

授权代表：_____ 联系电话：_____

地址：_____ 邮编：_____

被投诉人 1：

地址：_____ 邮编：_____

联系人：_____联系电话：_____

被投诉人 2

……

相关供应商：_____

地址：_____邮编：_____

联系人：_____ 联系电话：_____

二、投诉项目基本情况

采购项目名称：_____

采购项目编号：_____ 包号：_____

采购人名称：_____

代理机构名称：_____

采购文件公告:是/否 公告期限：_____

采购结果公告:是/否 公告期限：_____

三、质疑基本情况

投诉人于___年___月__日,向_____提出质疑，质疑事项为：

采购人/代理机构于___年___月___日,就质疑事项做出了答复/没有在法定期限内做出答复。

四、投诉事项具体内容

投诉事项 1：

事实依据：_____

法律依据：_____

投诉事项 2

……

五、与投诉事项相关的投诉请求

请求：_____

签字(签章)： 公章：

日期：

投诉书制作说明：

1.投诉人提起投诉时，应当提交投诉书和必要的证明材料，并按照被投诉人和与投诉事项有关的供应商数量提供投诉书副本。

2.投诉人若委托代理人进行投诉的，投诉书应按照要求列明“授权代表”的有关内容，并在附件中

提交由投诉人签署的授权委托书。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。

3.投诉人若对项目的某一分包进行投诉，投诉书应列明具体分包号。

4.投诉书应简要列明质疑事项，质疑函、质疑答复等作为附件材料提供。

5.投诉书的投诉事项应具体、明确，并有必要的事实依据和法律依据。

6.投诉书的投诉请求应与投诉事项相关。

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

附件 3：

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
2011 年 11 月 18 日

各省、自治区、直辖市人民政府，国务院各部委、各直属机构及有关单位：

为贯彻落实《中华人民共和国中小企业促进法》和《国务院关于进一步促进中小企业发展的若干意见》（国发〔2009〕36 号），工业和信息化部、国家统计局、发展改革委、财政部研究制定了《中小企业划型标准规定》。经国务院同意，现印发给你们，请遵照执行。

中小企业划型标准规定

一、根据《中华人民共和国中小企业促进法》和《国务院关于进一步促进中小企业发展的若干意见》（国发〔2009〕36 号)，制定本规定。

二、中小企业划分为中型、小型、微型三种类型，具体标准根据企业从业人员、营业收入、资产总额等指标，结合行业特点制定。

三、本规定适用的行业包括：农、林、牧、渔业，工业（包括采矿业，制造业，电力、热力、燃气及水生产和供应业），建筑业，批发业，零售业，交通运输业（不含铁路运输业），仓储业，邮政业，住宿业，餐饮业，信息传输业（包括电信、互联网和相关服务），软件和信息技术服务业，房地产开发经营，物业管理，租赁和商务服务业，其他未列明行业（包括科学研究和技术服务业，水利、环境和公共设施管理业，居民服务、修理和其他服务业，社会工作，文化、体育和娱乐业等）。

四、各行业划型标准为：

（一）农、林、牧、渔业。营业收入 20000 万元以下的为中小微型企业。其中，营业收入 500 万元及以上的为中型企业，营业收入 50 万元及以上的为小型企业，营业收入 50 万元以下的为微型企业。

（二）工业。从业人员 1000 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 300 万元及以上的为小型企业；从业人员 20 人以下或营业收入 300 万元以下的为微型企业。

（三）建筑业。营业收入 80000 万元以下或资产总额 80000 万元以下的为中小微型企业。其中，营业收入 6000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 300 万元及以上，且资产总额 300 万元及以上的为小型企业；营业收入 300 万元以下或资产总额 300 万元以下的为微型企业。

（四）批发业。从业人员 200 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 20 人及以上，且营业收入 5000 万元及以上的为中型企业；从业人员 5 人及以上，且营业收入 1000 万元及以上的为小型企业；从业人员 5 人以下或营业收入 1000 万元以下的为微型企业。

（五）零售业。从业人员 300 人以下或营业收入 20000 万元以下的为中小微型企业。其中，从业人员 50 人及以上，且营业收入 500 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（六）交通运输业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 3000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 200 万元及以上的为小型企业；从业人员 20 人以下或营业收入 200 万元以下的为微型企业。

（七）仓储业。从业人员 200 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（八）邮政业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人

员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（九）住宿业。从业人员 300 人以下或营业收入 6800 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十）餐饮业。从业人员 300 人以下或营业收入 6800 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十一）信息传输业。从业人员 2000 人以下或营业收入 68000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十二）软件和信息技术服务业。从业人员 300 人以下或营业收入 6800 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 50 万元及以上的为小型企业；从业人员 10 人以下或营业收入 50 万元以下的为微型企业。

（十三）房地产开发经营。营业收入 200000 万元以下或资产总额 6800 万元以下的为中小微型企业。其中，营业收入 1000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 100 万元及以上，且资产总额 2000 万元及以上的为小型企业；营业收入 100 万元以下或资产总额 2000 万元以下的为微型企业。

（十四）物业管理。从业人员 1000 人以下或营业收入 5000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 100 人及以上，且营业收入 500 万元及以上的为小型企业；从业人员 100 人以下或营业收入 500 万元以下的为微型企业。

（十五）租赁和商务服务业。从业人员 300 人以下或资产总额 120000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且资产总额 8000 万元及以上的为中型企业；从业人员 10 人及以上，且资产总额 100 万元及以上的为小型企业；从业人员 10 人以下或资产总额 100 万元以下的为微型企业。

（十六）其他未列明行业。从业人员 300 人以下的为中小微型企业。其中，从业人员 100 人及以上的为中型企业；从业人员 10 人及以上的为小型企业；从业人员 10 人以下的为微型企业。

五、企业类型的划分以统计部门的统计数据为依据。

六、本规定适用于在中华人民共和国境内依法设立的各类所有制和各种组织形式的企业。个体工商户和本规定以外的行业，参照本规定进行划型。

七、本规定的中型企业标准上限即为大型企业标准的下限，国家统计部门据此制定大中小微型企业的统计分类。国务院有关部门据此进行相关数据分析，不得制定与本规定不一致的企业划型标准。

八、本规定由工业和信息化部、国家统计局会同有关部门根据《国民经济行业分类》修订情况和企业发展变化情况适时修订。

九、本规定由工业和信息化部、国家统计局会同有关部门负责解释。

十、本规定自发布之日起执行，原国家经贸委、原国家计委、财政部和国家统计局 2003 年颁布的《中小企业标准暂行规定》国经贸中小企[2003]143 号同时废止。

第三章 评审程序、方法及标准

一、评审依据

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、财政部《政府采购竞争性磋商采购方式管理暂行办法》（财库[2014]214 号）；

4、财政部《财政部关于政府采购竞争性磋商采购方式管理暂行办法有关问题的补充通知》（财库[2015]124 号）；

5、财政部、工业和信息化部《政府采购促进中小企业发展管理办法》（财库[2020]46 号）；

6、财政部《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）；

7、财政部 2021 年 2 月 20 日发布《政府采购促进中小企业发展政策问答》；

8、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）；

9、《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）；

10、财政部《关于推动解决政府采购异常低价问题的通知》（财库〔2026〕2 号）；

11、政府采购相关法律法规及本项目采购文件。

二、磋商小组

1、采购人依法组建 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，其成员由从河南省政府采购专家库中随机抽取的评审专家和采购人代表共同组成，其中评审专家不得少于成员总数的三分之二。

2、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做出的评审意见无效。

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。原磋商小组所做出的评审意见无效。

3、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性、形式性、符合性审查，以确定其是否满足采购文件的实质性要求，并按照采购文件中规定的评审方法和标准，对符合性审查合格的响应文件进行评审。

三、评审原则

1、评审活动遵循公平、公正、科学和择优的原则。

2、对所有供应商的投标评定都采用相同的程序和标准。

3、评审由磋商小组负责。

四、评审纪律

1、磋商小组成员应当客观、公正地履行职责，遵守职业道德，对所提出的评审意见承担个人责任。

2、磋商小组成员不得向他人透漏对响应文件的评审和比较、成交候选人的推荐情况以及评审有关的其他情况。

3、在评审活动中，磋商小组成员不得擅离职守，影响评审程序正常进行。

4、磋商小组应当根据采购文件规定的评审标准和方法，对响应文件进行系统地评审和比较。采购文件中没有规定的标准和方法不得作为评审的依据。

5、在评审活动中，磋商小组成员不得与任何供应商或者与评审结果有利害关系的人进行私下接触，不得收受供应商、中介人、其他利害关系人的财物或者其他好处。

6、与供应商有利害关系的应主动回避。

7、参加评审的人员应严格遵守国家有关保密的法律、法规和规定，并接受有关部门的监督；

8、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，不得向他人透漏对响应文件的评审和比较、中标候选人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。

9、遵守法律、行政法规有关评审的相关规定。

五、评审过程的保密性

1、响应文件解密后，凡是与审查、澄清、评价和比较的有关资料以及授予合同建议等，参与评审的人员均不得向其他供应商及与评审无关的其他人员透露。

2、评审过程中，如果供应商试图向采购方或磋商小组成员施加任何不正当影响，都将导致其响应被拒绝。

六、评审要求

1、磋商小组对响应文件进行确认。

2、磋商小组推选组长，讨论、通过磋商工作流程和磋商要点。

3、磋商小组成员要依法独立评审，并对评审意见承担个人责任。磋商小组成员对需要共同认定的事项存在争议的，按照少数服从多数的原则做出结论。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并说明理由，否则视为同意。

4、磋商小组成员和评审工作有关人员不得干预或者影响正常评审工作，不得明示或者暗示其倾向性、引导性意见，不得修改磋商文件确定的评审程序、评审方法，不得征询采购人代表的倾向性意见，不得记录、复制或带走任何评审资料。成交候选人确定后，磋商小组不得修改评审结果或者要求重新评审，但因资格性审查认定错误或价格计算错误需依法重新评审的除外。应在评审报告中明确记载。

七、初步评审

1、初审内容通过资格性、形式性、符合性审查及实质性审查确定供应商是否符合采购文件规定，初步评审的要求及原则见本章附件一。

注：根据《关于促进政府采购公平竞争优化营商环境的通知》（财库〔2019〕38 号）的要求，采购人、采购代理机构对投标（响应）文件的格式、形式要求应当简化明确，不得因装订、纸张、文件排序等非实质性的格式、形式问题限制和影响供应商投标（响应）。

2、供应商所投所有货物和服务均应符合国家相关规定的要求，与采购文件有重大偏离的响应文件将被视为具有非实质响应性的响应文件而被拒绝。重大偏离系指响应文件的理解与采购文件中所述的采购内容、质量要求存在重大歧义的，或限制了采购人权力和供应商义务的规定，而纠正这些偏离将影响到其它提交实质性响应的供应商的公平竞争地位。

3、以下内容为采购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）磋商小组认为供应商的报价明显低于其他通过初步评审供应商的报价，使得其响应报价可能低于个别成本的，有可能影响服务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，磋商小组以低于成本报价竞标，其响应作为响应无效处理；

（2）不同供应商上传递交的电子响应文件制作机器码一致；

（3）不同供应商的响应文件相互混装；

（4）不同供应商的响应文件载明的项目管理成员或者联系人员为同一人。

注：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）的要求，磋商小组对异常低价的供应商投标（响应）情形，应当启动异常低价投标（响应）审查。

4、磋商小组对响应文件的判定，只依据响应文件内容本身，不依靠开启后的任何外来证明。

5、响应文件的澄清

5.1 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做出必要的澄清、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，响应文件报价出现前后不一致的，按照下列规定修正：

（1）响应文件中大写金额和小写金额不一致的，以大写金额为准；

（2）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；

（3）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，其响应无效。实质上没有响应采购文件要求的将被作为无效响应被拒绝。

5.2 提出的询问或澄清或要求其补充的材料。供应商必须按照采购方通知的时间在电子交易平台指定位置进行予以回应，该答疑和澄清均以书面方式进行回答，并根据电子交易平台的要求对上传的澄清文件电子签章。

5.3 供应商对响应文件的澄清仅针对磋商小组所提出的问题逐一进行回答或澄清，但不得改变报价价格及实质内容。

5.4 澄清将通过电子交易平台进行，供应商应按磋商小组的要求进行必要的澄清、说明或补正，并作为响应文件的一部分，具体操作详见（https://hnsggzyjy.henan.gov.cn/）公共服务-办事指南-河南省公共资源电子交易平台不见面服务系统使用指南。

八、竞争性磋商步骤

1、全过程电子化磋商

本次竞争性磋商采购采用全过程电子评审及磋商，供应商需在规定的时间内登录河南省公共资源交易中心远程登录本项目，根据电子交易平台的相关要求进行磋商、最后报价。所有程序及过程文件均在电子电子交易平台中记录并保存，如下述磋商过程与电子电子交易平台描述不一致，以电子电子交易平台相关模块及程序为准。

2、磋商

各供应商在线等候，磋商小组分别与通过初步评审的单一供应商分别进行磋商，并给予所有参加磋商的供应商平等的磋商机会。磋商过程和重要磋商内容均在电子电子交易平台内保存、记录，磋商小组根据磋商文件采购需求以及与各供应商磋商的结果，统一进行讨论，比较并提出修正意见。

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。

对磋商文件做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。

5、最后报价

磋商文件能够详细列明采购标的技术、服务要求的，磋商结束后，磋商小组应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。最后报价是供应商响应文件的有效组成部分。

请供应商注意电子交易平台要求提交的时间，在规定时间内没有提交最后报价的供应商，磋商小组视同放弃最后报价，其导致磋商未响应处理。未通过实质性响应的供应商将不再进行最后报价。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。

注：由于电子交易平台的特殊性，如要求供应商磋商最后报价为总价，那么，磋商首次报价中分项价格表的价格跟随供应商磋商最后报价的变化而优惠率变化调整计算。

若所有供应商的报价若超过了采购预算或响应文件中有采购人不能接受的条款时，采购人不能支付的或不能接受的，磋商活动终止；终止后，采购人需要采取调整采购预算或项目配置标准等，或采取其他采购方式的，应当在采购活动开始前获得财政部门批准。

6、评审方法及标准：

6.1 评审方法：本项目采用综合评分法，总分为 100 分。详细评审标准见本章附件二。

6.2 综合评分法，是指响应文件满足采购文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选人的评审方法。磋商小组按照磋商文件的要求和条件，根据各供应商的经济标（报价和价格）、商务标（履约能力）、技术标（服务水平）等各项因素作为评价的基础对磋商文件的响应

程度等进行综合评价、评分，将评审总得分按由高到低的顺序进行排列，并以此顺序推荐成交候选人。

6.3 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，按照技术指标优劣顺序推荐。

6.4 评审报告将由磋商小组全体人员签字或签章认可。

九、评审响应的最终评定和推荐成交候选人

1、磋商小组对供应商的最后报价和响应情况进行评估和比较。

2、评定原则及方法

2.1 最后报价不作为最终成交的唯一标准。

2.2 评审得分相同的，由采购人或者采购人委托磋商小组按照采购文件规定的方式确定供应商获得成交供应商推荐资格。

2.3 磋商小组将严格按照采购文件的规定和要求进行最终评定，并且对所有供应商都采用相同的程序和标准。

2.4 磋商小组将根据综合评分情况，按照评审总得分由高到低顺序排序，向采购人推荐 3 名成交候选人。

附件一、初步评审内容

1、响应文件的初审将按下表所述内容进行审查，无法满足的响应文件将按非实质性响应处理，各供应商及时根据河南省公共资源交易中心的要求补充及完善其市场主体信息库中相应内容。有利于评审选取。

2、供应商根据采购文件的规定，使用电子交易平台提供的“响应文件制作工具”进行编制响应文件，磋商小组将根据本表所述内容进行评审，未通过初步评审的供应商的响应文件做无效响应处理。

评审项目	评审原则
资格性审查	第六章 竞争性磋商响应文件格式 一商务部分 1 资格证明文件 （1）具备独立承担民事责任的能力法人资格 （2）具有良好的商业信誉和健全的财务会计制度 （3）有依法缴纳税收和社会保障资金的良好记录 （4）履行合同所必需的货物和专业技术能力的书面声明 （5）在经营活动中没有重大违法违规记录的书面声明 （6）无不良信用记录承诺 （7）无行政及经济关联或利害关系的承诺 （8）政府采购政策落实 （以上须提供相关证明见供应商须知前附表 16.1） 内容是否提供、是否齐全、有效、符合采购文件要求
	在“信用中国”网站(www. creditchina. gov.cn)和“中国政府采购网”(www.ccgp.gov.cn)查询，未被列入失信被执行人、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。
形式性审查	第六章 竞争性磋商响应文件格式， 内容是否响应、是否符合采购文件要求
符合性审查	第六章 竞争性磋商响应文件格式 中的签署、盖章， 是否提供、是否齐全、有效、符合采购文件要求
	第六章 竞争性磋商响应文件格式 一商务部分 2 法定代表人身份证明或授权委托书， 内容是否提供、是否齐全、有效、符合采购文件要求
	第六章 竞争性磋商响应文件格式 一商务部分 3 报价函、分项价格表内容， 是否填写或提供、是否有效、符合采购文件要求
实质性条款	第六章 竞争性磋商响应文件格式 一商务部分 4 商务条款响应与偏离表，或不满足本磋商文件中标注“★”的实质性条款要求的， 是否响应，是否存在严重偏离，是否符合采购文件要求
其他	是否存在采购人不可接受的条件，是否存在与法律规章规定有不符的其他规定要求

附件二、详细评审标准

评委将根据评分标准，分别对通过符合性审查、资格性审查的供应商，进行综合评分。具体评分标准如下：

评分类型	评分因素	要素分值	评分细则
价格	报价	20	（1）满足磋商文件要求且最终报价最低的供应商的报价（单日服务费报价）为

			磋商基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算： 磋商报价得分=（磋商基准价/最后磋商报价）×价格权值（20%）×100 （2）最终得分计算保留小数点后两位，四舍五入。 注：专门面向中小企业采购的项目，不再执行价格评审优惠的扶持政策。 满足磋商文件要求指：通过初步评审和最终报价的总报价未超过预算金额的供应商。价格评分按照供应商单日服务费报价进行评审。
履约能力27分	企业证书8分	6	（1）具有 ISO9001 质量管理体系认证证书，其中包含计算机应用软件和计算机信息系统集成内容的得 1 分； （2）具有 ISO27001 信息安全管理体系认证证书的得 1 分； （3）具有中国网络安全审查技术与认证中心（中国信息安全认证中心）认证的三级（含）以上软件安全开发服务资质或信息系统安全运维服务资质或信息系统安全集成服务资质或信息安全应急处理服务资质的，每有一项资质得 1 分，最高得 4 分。 注：需提供以上有效的证书扫描件并加盖供应商公章，未提供本项内容或者其它情况得 0 分。
		2	进行等级保护的测评工作时，供应商具备公安等国家主管部门认可的等保测评服务资质或由具备公安等国家主管部门认可的等保测评服务资质的单位协助进行的，得 2 分。 注：需提供以上有效的证书或服务承诺函扫描件并加盖供应商公章，未提供本项内容或者其它情况得 0 分。
	成功案例7分	4	具有 2023 年至今类似信息安全项目业绩合同，提供一份得 1 分，最高得 4 分。 注：需提供以上有效的合同及发票扫描件并加盖供应商公章，未提供本项内容或者其它情况得 0 分。
		3	供应商提供类似行业用户针对拟投入本项目的工具质量稳定或无质量问题证明材料，每提供一份得 1 分，最多得 3 分。 注：需提供以上有效的证明材料扫描件并加盖供应商公章，未提供本项内容或者其它情况得 0 分。
	服务团队实力12分	12	（1）提供一线驻场服务人员 3 人,二线非驻场服务人员不少于 5 人的技术服务人员得 3 分，在满足以上配置的条件下，一线驻场服务人员每再增加 1 人加 2 分；二线非驻场服务人员每再增加 1 人加 1 分，此项共计最高得 7 分。 （2）服务人员具有国家行政主管部门颁发的计算机技术和软件专业技术资格（水平）（系统集成、软件开发和网络安全）资格证书的，每提供 1 份证书得 1 分，最高得 5 分。 注：需提供以上有效的人员工作简历（包括工作时间、承担工作内容、证明人联系方式等内容）的证明材料和相关证书扫描件并加盖供应商公章，未提供本项内容或者其它情况得 0 分。
服务水平53分	项目需求理解	7	针对项目概况、服务内容、目标、范围的需求有清晰理解、分析详细： 1、有完整、全面详细描述的得 7 分； 2、有较为完整描述的得 5 分；

			3、有简单描述的得 3 分； 4、内容过于简单、有欠缺或不充分的得 1 分； 5、未提供本项内容或者其它情况得 0 分。
	技术实施方案	8	针对项目建设需求、服务实施组织（包括但不限于服务具体内容、服务标准、实施管理、防护措施、技术和设备配置、系统优化、关键点和难点处理、风险管理等内容）： 1、有完整、全面详细描述的得 8 分； 2、有较为完整描述的得 6 分； 3、有简单描述的得 4 分； 4、内容过于简单、有欠缺或不充分的得 2 分； 5、未提供本项内容或者其它情况得 0 分。
	进度管理	5	针对服务实施时间（包括但不限于时间计划、进度管理、实施管理等内容）： 1、有完整、全面详细描述的得 5 分； 2、有较为完整描述的得 3 分； 3、有简单描述的得 2 分； 4、内容过于简单、有欠缺或不充分的得 1 分； 5、未提供本项内容或者其它情况得 0 分。
	技术服务响应	15	针对技术服务指标要求所有项逐条进行响应，不能漏项，全部满足的得 15 分。标注★的为实质性要求，每有一项不满足为无效投标，不带“★”指标为一般指标，每有一项不满足扣 0.5 分，扣完为止。 注：对技术参数进行夸大或响应不实者，用户有权追究其因此造成的损失或责任。
	运营维护方案	8	针对运营维护服务范围和要求内容（包括但不限于服务内容、组织管理、人员管理、制度管理、质量管理、部件保障、系统优化、技术培训、紧急预案、关键点和难点处理等内容）： 1、有完整、全面详细描述的得 8 分； 2、有较为完整描述的得 6 分； 3、有简单描述的得 4 分； 4、内容过于简单、有欠缺或不充分的得 2 分； 5、未提供本项内容或者其它情况得 0 分。
	安全保密	5	针对根据项目需求制订的安全保密措施（包括但不限于安全保密、网络安全、数据安全的方式、内容、工作中需要注意的事项等内容）： 1、有完整、全面详细描述的得 5 分； 2、有较为完整描述的得 3 分； 3、有简单描述的得 2 分； 4、内容过于简单、有欠缺或不充分的得 1 分； 5、未提供本项内容或者其它情况得 0 分。
	验收方案	5	针对根据对项目验收的要求，结合自身同类项目经验，制定详细的验收方案（包括但不限于验收方式、验收时间、验收流程、验收依据、验收标准、验收文档

			和以及验收过程中可能出现的问题及问题补措施等内容）： 1、有完整、全面详细描述的得 5 分； 2、有较为完整描述的得 3 分； 3、有简单描述的得 2 分； 4、内容过于简单、有欠缺或不充分的得 1 分； 5、未提供本项内容或者其它情况得 0 分。
总分		100	

价格扣除原则：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磋商基准价和最后磋商报价。本次专门面向中小企业采购的项目，不再执行价格评审优惠的扶持政策。

对磋商报价、商务、技术响应得分的汇总，作为该供应商的最后得分。评分及计算结果均保留小数点后两位，四舍五入。

异常低价投标（响应）审查：

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）采购人应当在采购文件中明确，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 65%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×65%

（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 65%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×65%

（3）投标（响应）报价低于采购项目最高限价 65%的，即投标（响应）报价<采购项目最高限价×65%；

（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。

采购人可以结合具体项目实际情况，提高上述第 1 项至第 3 项中启动异常低价投标（响应）审查的数值标准，但是最高不得超过 65%。

相关法律法规对供应商报价有规定的，从其规定。

评审委员会启动异常低价投标（响应）审查后，属于前述第 1 项至第 4 项情形的，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。

第四章 合同草案及主要条款

合同编号：

河南省福利彩票发行中心(河南省养老事业发展中心)
信息安全服务项目合同

甲　　方：河南省福利彩票发行中心(河南省养老事业发展中心)
乙　　方：_____
签订地点：_____
签订日期：_____

甲方：河南省福利彩票发行中心(河南省养老事业发展中心)

地址：　　邮政编码：

联系人：　　E-mail：

电话：　　传真：

乙方：

地址：　　邮政编码：

联系人：　　E-mail：

电话：　　传真：

根据《中华人民共和国民法典》、《中华人民共和国政府采购法》等相关法律法规之规定，就项目名称为_____，按照平等、自愿、公平和诚实信用的原则，经甲乙双方协商一致，约定以下合同条款，以兹共同遵守、全面履行。

第一条：合同项目与定义

1.1　本合同所称“安全服务”内容指：信息安全服务，涵盖河南省福利彩票发行中心(河南省养老事业发展中心)生产一机房、生产二机房、数据管理中心三个机房和生产系统（含电脑票热线销售系统和即开票销售系统）、计算机辅助管理系统（CAM）（含运营管理信息系统（OMIS）、办公自动化（OA）和渠道营销管理平台）、门户网站系统（河南福彩网）三个系统，并且具有可扩展性，能够满足后期信息系统安全建设的要求。同时本项目采购人（即甲方）所购买的是安全服务，所需要提供的软硬件系统及设备归属成交供应商（即乙方）所有。除非明确注明，本合同所涉及以上安全服务内容下面统称为“安全服务”。

1.2　本合同中“双方”仅指本合同的缔约方，即上述甲方和乙方。

1.3　合同文件：

（1）本合同条款及其补充合同、变更协议；

（2）中标通知书；

（3）招标文件；

（4）中标单位投标文件；

（5）其他。

上述所指合同文件应认为是互相补充和解释的，但是有模棱两可或互相矛盾之处，以其所列内容顺序为准。

第二条：服务的内容和范围

从河南省福利彩票发行中心(河南省养老事业发展中心)的实际情况出发，采用安全服务托管方式，

建立起河南福彩综合防控服务体系，以满足国家相关法律法规和福彩行业的要求，同时又满足河南福彩实际业务的需求。

2.1 总体服务内容和范围

序号	项目名称	项目内容	金额（元）
1	销售网络基础安全防控服务	建立覆盖全省的销售网络基础安全防控服务平台，通过平台为各业务区提供综合防控服务，符合行业安全建设的要求。包括但不限于建设态势感知平台、威胁情报联防平台、销售网点运维管理平台等专用平台及配套的服务，满足等级保护的要求。	
2		核心业务区安全防控服务：通过基础安全防控服务平台，为核心业务区提供相关工具和防控服务，符合行业安全建设的要求。包括但不限于电脑票、即开票等销售系统的综合防控，满足等级保护的要求。	
3		辅助业务区安全防控服务：通过基础安全防控服务平台，为辅助业务区提供相关工具和防控服务，符合行业安全建设的要求。包括但不限于中福彩中心、各级福彩机构、销售网点等业务接入管理，满足等级保护的要求。	
4		外联业务区安全防控服务：通过基础安全防控服务平台，为外联业务区提供相关工具和防控服务，符合行业安全建设的要求。包括但不限于银行、运营商、新渠道等外联单位的业务接入管理，满足等级保护的要求。	
5		外部办公区安全防控服务：通过基础安全防控服务平台，为外部办公区提供相关工具和防控服务，符合行业安全建设需要。包括但不限于外部办公业务、互联网业务等安全接入管理，满足等级保护的要求。	
6	销售网络安全加固服务	提供覆盖全省的销售网络安全加固服务，通过提供相关工具和防控服务，建设符合行业安全的要求。包括但不限于防火墙、入侵防御、漏洞扫描、网络审计、数据库审计、日志审计、WEB 应用防火墙、高级持续性威胁检测与管理系统、防病毒、准入系统、堡垒机等通用安全设备及配套的服务，满足等级保护的要求。	
7	销售网点综合安全接入服务	提供覆盖全省的销售网点综合安全接入服务，通过提供相关工具和防控服务，建设符合行业安全的要求，包括但不限于对现有“综合业务安全接入系统”中心设备及全省传统销售网点已部署终端设备的运营维护，以及涵盖全省渠道销售网点的安全接入，满足等级保护的要求。	
8	年度等级保护测评服务	完成生产系统（含电脑票热线销售系统和即开票销售系统）、计算机辅助管理系统（CAM）（含运营管理信息系统（OMIS）、办公自动化（OA）和渠道营销管理平台）、门户网站系统（河南福彩网）三个系统的年度等保定级、测评，以及在公安部门的备案等相关工作，满足等级保护的要求及行业安全建设的要求。	
9	年度驻场运营维护服务	专项攻防演练保障服务：在服务期内，根据公安部门、民政部门及中福彩中心等行业主管部门的要求，提供配合开展专项安全检查进行的	

		攻防演练等配套服务工作，提供现场服务保障，具体保障时间与行业主管部门的要求一致。	
10		系统安全运维驻场服务：针对本项目涉及的系统提供人员驻场服务，包括但不限于对中心机房和销售网点提供定期巡检、安全检查、应急响应等运维服务，以及对软件工具、病毒库、漏洞库和特征库等进行升级迭代跟踪及更新服务。	

注：安全服务包括提供相应安全服务所需的平台软硬件部署、扩容、优化升级服务和服务周期内相应的运营服务，其中包括不少于 2 次漏洞扫描和 1 次渗透测试。

其中，合同签订生效之日起 30 日内，完成上表中 1-7 项所约束的安全服务平台建设及安装或升级服务，同时服务期内提供维护维保、相应的安全运营服务等。

2.2 运营维护服务范围

序号	类别	名称	规格型号	生产厂商	数量
1	中心设备	TSAS 硬件平台	TSAS-1000	西安天泰创新科技有限公司	2 台
2		安全管理中心和安全注册认证中心	TRM-1000HN	西安天泰创新科技有限公司	2 块
			天泰 TSM 安全管理软件[简称：TSM]V1.0)	西安天泰创新科技有限公司	2 套
			天泰 TRM 安全注册认证软件[简称：TRM]V1.0	西安天泰创新科技有限公司	2 套
3		业务均衡网关	TBG-1000HN	西安天泰创新科技有限公司	2 块
			天泰业务均衡软件[简称：TBG]V1.0)	西安天泰创新科技有限公司	2 套
4		安全接入中心	TSG-1000HN	西安天泰创新科技有限公司	2 块
			天泰安全接入软件[简称：TSG/C]V2.0	西安天泰创新科技有限公司	2 套
5		防火墙	SGFW-T1-2000P	上海天泰网络技术有限公司	1 台
		防火墙	TNFW-2000P	西安天泰创新科技有限公司	1 台
6	终端设备	终端用户接入服务管理器	TSG-100HN	西安天泰创新科技有限公司	4300 台
			天泰安全接入软件[简称：TSG/C]V1.0	西安天泰创新科技有限公司	4300 套

2.3 运营维护服务要求

通过定期对“综合业务安全接入系统”中心及终端设备进行检查、检修和维护，确保系统安全运行。

（1）在服务期内，乙方应提供7*24小时的维护维保服务，在接到甲方报修通知后，服务人员持续跟进直到故障排除后设备完全恢复正常使用为止。特殊情况下乙方应提供备用设备，确保服务范围内所约定的软硬件系统正常运转。遇到重大技术问题，及时组织有关技术专家进行会诊，并采取相应措施以确保正常运行。

（2）在服务期内，乙方应严格要求服务人员不得使用不符合技术要求和质量要求的零配件，同时认真做好服务记录，记录维修前故障和修理后的设备质量状况；维修完毕，请甲方检验修理后的设备和服务记录。

（3）乙方应保证常用维修配件的合理储备，确保维护维保工作的正常进行，避免因缺少零配件而延误维修时间。

（4）当服务范围内所约定的软硬件系统发生故障时，乙方应及时进行设备维修与更换。乙方应设立备件库进行备件支持，对故障件维修并及时更换不能现场修复的设备。

（5）乙方应根据维护维保服务记录，定期提交服务报告，归类总结服务期内的故障和甲方提出的问题，对于带有普遍性的问题及时予以重点解决，同时乙方应定期进行维护巡检，以及时发现并处置故障。

（6）乙方应根据甲方需求定期提供健康检查、系统巡检、专项维护等服务，并通过监测和分析，及时发现设备中存在的问题和隐患。针对隐患，乙方采取防范措施加以预防；针对发现的问题，应果断采取处置措施；最后提交相应的服务报告。

（7）乙方应根据甲方需求进行软件升级和健壮性配置优化；所有软件优化升级必须按照甲方要求先进行部分销售网点测试，测试成功后再进行全省销售网点的优化升级。

（8）乙方应根据甲方要求进行相关技术培训。

（9）乙方所有技术操作应获得甲方授权后执行。

（10） 乙方应提供日常维护及应急响应服务。

第三条：双方的权利和义务

（一）甲方的权利和义务

3.1 甲方采用“购买服务”模式，由乙方提供建立河南福彩综合防控服务体系所需的设备、工具和人员等服务。

3.2 甲方应向乙方提交甲方执行本合同的联系人、信息安全负责人和相关管理甲方网络、设备和应用系统的人员名单和联系方式，并在上述信息发生变化时及时通知乙方。

3.3 除非双方另有书面约定，甲方承认乙方向甲方提供的相关设备、软件等的所有权及知识产权属于乙方，甲方无权复制、传播、转让、许可或提供他人使用这些资源。

3.4 甲方应按时向乙方交纳本合同约定的费用。

3.5 甲方若发现遭遇黑客攻击、病毒感染等情况时，应及时通知乙方，并协助乙方进行排查、阻断和必要的紧急措施。在未完全解除黑客攻击、病毒感染等情况时，甲方需要自行备份系统、数据并暂停相关外部服务，待解除黑客攻击、病毒感染后再恢复外部服务。

3.6 甲方服务范围、内容发生变化时，应及时通知乙方，并征得乙方书面同意后，方可要求乙方提供相应的服务，必要时双方签订补充合同。

（二）乙方的权利和义务

3.7 按照本合同的规定为甲方提供相应的“安全服务”。

3.8 为甲方提供建立河南福彩综合防控服务体系所需的设备、工具和人员等服务。

3.9 除非双方另有书面约定，甲方提供给乙方的相关资料、数据和文件等的知识产权归属甲方，乙方在甲方许可下使用该资源，且需要注意相关资料的保密工作。

3.10 按照本合同收取相关费用。

3.11 乙方若发现甲方遭遇黑客攻击、病毒感染等情况时，应及时通知甲方，并安排人员进行排查、阻断和必要的紧急措施。乙方应保持提供的设备、工具等相关特征库、病毒库及时更新。

3.12 乙方必须设有7*24小时的热线电话，提供7*24小时不间断的高质量服务，并且提供3名驻场工程师。同时根据甲方需求提供现场技术支持,一旦接到甲方现场技术支持请求，即派经验丰富的专业工程师以最短的时间内到达现场服务，进行安全检测、定位、维护，尽快恢复甲方系统正常运行。同时建立规范的服务文档管理信息系统，必须有规范的服务文档管理如信息安全服务记录与阶段总结报告等材料作保障。

3.13 甲方服务范围、内容发生变化时，乙方在力所能及的范围内积极配合，若相关的服务超出乙方服务范围，乙方有权要求签订补充合同。

第四条：服务期、服务费用及支付方式

4.1 服务期

本合同的安全服务平台的交付期：合同签订生效之日起30日内完成安全服务平台建设及安装或升级服务并交付使用。

本合同的安全服务平台后续运营服务期：不少于365天，具体服务周期以总预算除以单日服务费报价后取整位数确定。

4.2 服务费用

本合同总价为：￥ 元（大写： ）。

4.3 支付方式

本合同签订后，于服务起始日前二十个工作日内,乙方向甲方支付合同价款3%的履约保证金（履约保证金户名：河南省福利彩票发行中心(河南省养老事业发展中心)，账号：246801819248，开户行：中国银行郑州金水支行营业部）。甲方在收到履约保证金且乙方出具合法发票后十五个工作日内，甲方向乙方支付合同总价款的100%。待维护期满（按日历计算）后三十个工作日内，甲方向乙方一次性无息返还3%的履约保证金。发票是付款的先决条件，如乙方无提供发票，甲方有权拒绝支付合同款。

第五条：合同生效、解除、终止及违约责任

5.1 本合同经双方法人代表或授权代表签字并由合同主体盖章后生效。如果在合同生效期间或期满之后甲方需要乙方的其他服务，双方另行签订合同。

5.2 本合同在下述情形下终止，终止方应书面通知另一方：

5.2.1 一方当事人主体资格消失，如破产。但进行重组、名称变更或者与第三方合并等不在此列。

5.2.2 根据本合同的约定解除本合同。

5.2.3 因不可抗力而解除本合同或者双方当事人协商一致解除本合同的。

5.2.4 依法律、法规规定的情形而终止。

5.3 本合同到期后，如果甲方没有按时支付续约款项，则双方认同本合同执行终止。乙方届时将关

闭并撤离设备、工具及服务人员。关闭并撤离设备、工具及服务人员期间或以后，若甲方遭遇黑客攻击、病毒感染等情况时，乙方不负任何责任。

5.4　除不可抗力外，如果乙方没有按照本合同约定的期限、地点和方式履行，那么甲方可要求乙方支付违约金，违约金按每迟延履行一日的应提供而未提供服务价格的0.5%计算，最高限额为本合同总价的10 %；迟延履行的违约金计算数额达到前述最高限额之日起，甲方有权在要求乙方支付违约金的同时，书面通知乙方解除本合同。

5.5　除不可抗力外，如果甲方没有按照本合同约定的付款方式付款，乙方可要求甲方支付违约金，违约金按每迟延付款一日的应付而未付款的0.5%计算，最高限额为本合同总价的10%；迟延付款的违约金计算数额达到前述最高限额之日起，乙方有权在要求甲方支付违约金的同时，书面通知甲方解除本合同。因财政部门等非甲方原因造成延期支付的，不视为甲方违约，无需承担责任。

5.6　任何一方按照前述约定要求违约方支付违约金的同时，仍有权要求违约方继续履行合同、采取补救措施，并有权按照己方实际损失情况要求违约方赔偿损失；任何一方按照前述约定要求解除本合同的同时，仍有权要求违约方支付违约金和按照己方实际损失情况要求违约方赔偿损失；且守约方行使的任何权利救济方式均不视为其放弃了其他法定或者约定的权利救济方式。

第六条：责任限制

6.1　因乙方原因造成甲方与第三方纠纷的，乙方负责解决并赔偿甲方因此遭受的损失。因甲方原因造成乙方与第三方纠纷的，甲方负责解决并赔偿乙方由此遭受的全部损失。

6.2　因乙方原因导致安全服务不及时或者未履行信息安全服务责任造成的故障每月累计超过6小时，乙方应对本合同约定的服务免费延长一个月。年累计超过5天，甲方则有权终止合同，乙方须在五日内退回剩余款项并且支付甲方本合同总价30%的赔偿款。

6.3　乙方应甲方要求，邀请第三方公司协助进行服务时，若发生由于受邀第三方公司操作不慎造成损失的，乙方不负任何法律责任。

第七条：争议解决

7.1　因履行本合同或与本合同有关的一切争议，双方当事人应通过友好协商方式解决。

7.2　如果协商未成，双方同意应向甲方所在地人民法院起诉。

第八条：不可抗力

8.1　任何一方遇有不可抗力而全部或部分不能履行本合同或迟延履行本合同，应自不可抗力事件发生之日起五日内，将事件情况以书面形式通知另一方，并于事件发生之日起二十日内，向另一方提交导致其全部或部分不能履行或迟延履行的证明。

8.2　遭受不可抗力的一方应采取一切必要措施减少损失，并在事件消除后立即恢复本合同的履行，除非此等履行已不可能或者不必要。

8.3　本条所称“不可抗力”系指不能预见、不能避免或不能克服的客观事件，包括但不限于自然灾害如洪水、火灾、爆炸、雷电、地震和风暴等以及社会事件如战争、动乱、政府管制、国家政策的突然变动和罢工等。

第九条：保密

任何一方对在本合同履行过程中以任何方式获知的另一方商业秘密或其他技术及经营信息均负有保密义务，不得向任何其他第三方透露或泄露，但中国现行法律、法规另有规定或经双方书面同意的除外。

第十条：合同的解释、法律适用及其他

10.1 本合同的解除、终止或者本合同有关条款的无效均不影响本合同关于合同的解释、违约责任、知识产权、法律适用、责任限制、补偿及争议解决的有关约定的效力。

10.2 在本合同有效期内，因乙方上市、被收购、与第三方合并、名称变更等事由，甲方同意乙方可以将其在本合同中的权利和/或义务转让给相应的乙方权利/义务的承受者，但乙方应保证甲方在本合同中的权益不会因此而受到不利影响。

10.3 本合同的有关条款或者约定若与双方以前签署的有关条款或者乙方的有关陈述不一致或者相抵触的，以本合同为准。

10.4 本合同正本一式肆份，甲方贰份，乙方贰份。

10.5 本合同未尽事宜，甲乙双方另签订补充合同，补充合同与本合同具有同等法律效力。

甲方（盖章）：河南省福利彩票发行中心(河南省养老事业发展中心)

授权代表或法人代表（签字）：

住所地：河南郑州

签订日期：

乙方（盖章）：

授权代表或法人代表（签字）：

住所地：

开户名称：

开户银行：

帐号：

签订日期：

第五章 采购需求和服务要求

（一）项目概况

自《网络安全法》施行以来，从2020年起省中心每年通过服务购买的形式建成了“主动防御”的安全架构，建立了一个安全防护体系，保障信息中心的业务安全、数据安全和管理安全。同时根据《中共河南省福利彩票发行中心委员会会议纪要【2026】3号》文件精神内容，现就河南省福利彩票发行中心(河南省养老事业发展中心)信息安全服务项目继续进行政府采购。服务范围和服务要求如下：

1) 服务范围：提供信息安全服务（包括必要的软硬件工具配套），涵盖河南省福利彩票发行中心(河南省养老事业发展中心)生产一机房、生产二机房、数据管理中心三个机房和生产系统（含电脑票热线销售系统和即开票销售系统）、计算机辅助管理系统（CAM）（含运营管理信息系统（OMIS）、办公自动化（OA）和渠道营销管理平台）、门户网站系统（河南福彩网）三个系统，并且具有可扩展性。

2) 服务要求：首先对河南福彩信息中心网络和应用进行安全域划分，将业务外网和生产内网分开，并进一步细化为外部办公区、外部业务区、内部服务区和核心业务区等，并根据不同的业务类型制定不同的安全建设方案。另外，对现有安全体系和安全策略进行优化和调整，并根据按照《信息系统安全等级保护测评要求》（GB/T22239-2019）等政策文件的新要求补充新的安全措施和安全防护手段。

（二）采购项目预（概）算

总 预 算：190.00万元

包1预算：190.00万元

包2预算：无

（三）采购标的汇总表

包号	序号	标的名称	品目 分类编码	计量 单位	数量	是否进口
包1	1	2026年度河南省福利彩票发行中心(河南省养老事业发展中心）信息安全服务项目	运行维护服务 C16070000	个	1	否

（四）技术商务要求

1.技术要求

1.1 项目概况

（1）项目背景

随着福彩销售网点的兼营化和社会化，彩票各种信息管理系统也变得复杂化和多样化，而且随着《网络安全法》的颁布，新的等级保护制度（等级保护2.0）的施行，对河南福彩的信息化管理又提出了更高的要求。例如等级保护2.0要求技术和管理两方面都要进行完善，所以信息安全管理工作需要专业的信息安全技术人员作为支撑，包括安全评估、安全加固、应急响应等方面。

面对省中心各种业务信息系统越来越复杂，而且不同类型彩票销售网点数量也在逐年增加，仅仅依靠传统的人工安全管理手段，无法满足复杂的业务信息系统管理要求。同时河南福彩信息安全工作是需

要每年持续建设的，省中心从实际情况出发，采用信息安全服务托管方式。从2020年起省中心每年通过服务购买的形式建成了“主动防御”的安全架构，建立了一个安全防护体系，保障信息中心的业务安全、数据安全和管理安全。同时根据《中共河南省福利彩票发行中心委员会会议纪要【2026】3号》文件精神内容，现就河南省福利彩票发行中心(河南省养老事业发展中心)信息安全服务项目继续进行政府采购。

（2）项目目标

通过采购及时、高效、全方位的安全服务建立起河南福彩综合防控服务体系，以满足国家相关法律法规和福彩行业的要求，同时又满足河南福彩实际业务的需求。

（3）项目内容

本次安全服务托管要求一线驻场服务人员3人，服务期限:不少于365天，具体服务周期以总预算除以单日服务费报价后取整位数确定。服务范围和服务要求如下：

1) 服务范围：提供信息安全服务（包括必要的软硬件工具配套），涵盖河南省福利彩票发行中心(河南省养老事业发展中心)生产一机房、生产二机房、数据管理中心三个机房和生产系统（含电脑票热线销售系统和即开票销售系统）、计算机辅助管理系统（CAM）（含运营管理信息系统（OMIS）、办公自动化（OA）和渠道营销管理平台）、门户网站系统（河南福彩网）三个系统，并且具有可扩展性。

2) 服务要求：首先对河南福彩信息中心网络和应用进行安全域划分，将业务外网和生产内网分开，并进一步细化为外部办公区、外部业务区、内部服务区和核心业务区等，并根据不同的业务类型制定不同的安全建设方案。另外，对现有安全体系和安全策略进行优化和调整，并根据按照《信息系统安全等级保护测评要求》（GB/T 22239-2019）等政策文件的新要求补充新的安全措施和安全防护手段。

（4）安全服务内容一览表

序号	项目名称	项目内容	服务期	时间	地点
1	销售网络基础安全防控服务	建立覆盖全省的销售网络基础安全防控服务平台，通过平台为各业务区提供综合防控服务，符合行业安全建设的要求。包括但不限于建设态势感知平台、威胁情报联防平台、销售网点运维管理平台等专用平台及配套的服务，满足等级保护的要求。	不少于365天，具体服务周期以总预算除以单日服务费报价后取整位数确定	合同签订生效之日起30天内完成平台建设和工具部署并交付使用	河南省福利彩票发行中心(河南省养老事业发展中心)指定点（包括但不限于省中心机房
2		核心业务区安全防控服务：通过基础安全防控服务平台，为核心业务区提供相关工具和防控服务，符合行业安全建设的要求。包括但不限于电脑票、即开票等销售系统的综合防控，满足等级保护的要求。			
3		辅助业务区安全防控服务：通过基础安全防控服务平台，为辅助业务区提供相关工具和防控服务，符合行业安全建设的要求。包括但不限于中福彩中心、各级福彩机构、销售网点等业务接入管理，满足等级保护的要求。			

4		外联业务区安全防控服务：通过基础安全防控服务平台，为外联业务区提供相关工具和防控服务，符合行业安全建设的要求。包括但不限于银行、运营商、新渠道等外联单位的业务接入管理，满足等级保护的要求。			及全省各地市销售网点）
5		外部办公区安全防控服务：通过基础安全防控服务平台，为外部办公区提供相关工具和防控服务，符合行业安全建设需要。包括但不限于外部办公业务、互联网业务等安全接入管理，满足等级保护的要求。			
6	销售网络安全加固服务	提供覆盖全省的销售网络安全加固服务，通过提供相关工具和防控服务，建设符合行业安全的要求。包括但不限于防火墙、入侵防御、漏洞扫描、网络审计、数据库审计、日志审计、WEB 应用防火墙、高级持续性威胁检测与管理系统、防病毒、准入系统、堡垒机等通用安全设备及配套的服务，满足等级保护的要求。			
7	销售网点综合安全接入服务	提供覆盖全省的销售网点综合安全接入服务，通过提供相关工具和防控服务，建设符合行业安全的要求，包括但不限于对现有“综合业务安全接入系统”中心设备及全省传统销售网点已部署终端设备的运营维护，以及涵盖全省渠道销售网点的安全接入，满足等级保护的要求。			
8	年度等级保护测评服务	完成生产系统（含电脑票热线销售系统和即开票销售系统）、计算机辅助管理系统（CAM）（含运营管理信息系统（OMIS）、办公自动化（OA）和渠道营销管理平台）、门户网站系统（河南福彩网）三个系统的年度等保定级、测评，以及在公安部门的备案等相关工作，满足等级保护的要求及行业安全建设的要求。			
9	年度驻场运营维护服务	专项攻防演练保障服务：在服务期内，根据公安部门、民政部门及中福彩中心等行业主管部门的要求，提供配合开展专项安全检查进行的攻防演练等配套服务工作，提供现场服务保障，具体保障时间与行业主管部门的要求一致。			
10		系统安全运维驻场服务：针对本项目涉及的系统提供人员驻场服务，包括但不限于对中心机房和销售网点提供定期巡检、安全检查、应急响应等运维服务，以及对软件工具、病毒库、漏洞库和特征库等进行升级迭代跟踪及更新服务。			

1.2 对投标文件的基本要求

（1）供应商应按照招标文件的相关规定编制投标文件，投标文件应针对项目需求中的各项要求逐条或分块做出实质性响应，其响应情况作为评审的重要依据。**招标文件中标注★的要求为实质性要求，供应商须完全响应且不允许存在负偏离，否则将导致其投标无效。**

（2）投标文件应包含但不限于以下技术服务方案或资料，以下方案或资料将作为项目评审的重要依据：

1）供应商应在充分理解招标文件中描述的用户需求的基础上，根据招标文件有关章节提供的材料以及对采购人所需服务情况的了解，提供对本项目的理解和详细描述。

2）人员配备。供应商应提供就本项目投入技术人员的名单、简历以及相关资质证书、证明资料等。

3）技术实施方案。供应商应按照招标文件要求详细阐述项目实施方案，根据项目范围重点阐述本项目安全服务具体内容、服务标准、实施管理、技术和设备配置、系统优化、关键点和难点处理、防护措施、风险管理等。

4）进度管理。供应商必须按照本项目技术需求详细阐述管理方案，内容包括项目时间计划、进度管理、实施管理等。

5）技术服务指标响应。供应商必须按照本项目技术指标要求对应详细不能漏项响应或阐述，内容包括安全防控服务、安全加固服务、安全接入服务、等级保护测评服务专项攻防演练保障服务、运维驻场服务等。

6）运营维护服务。供应商必须按照本项目技术需求详细阐述运维服务方案，内容包括服务内容、组织管理、人员管理、制度管理、质量管理、部件保障、系统优化、技术培训、紧急预案、应急响应流程、关键点和难点处理等。

7）安全保密。供应商应根据对河南福彩综合防控的了解，制定安全保密、网络安全措施。内容包括：安全保密、网络安全、数据安全的方式、内容、工作中需要注意的事项等。

8）验收方案。供应商应根据招标人对项目验收的要求，制定详细的验收方案。验收方案内容包括但不限于验收方式、验收时间、验收流程、验收依据、验收标准、验收文档和以及验收过程中可能出现的问题及应对措施等。

1.3 项目实施要求

（1）项目建设需求

1）需要满足信息中心建设发展

本项目所提供的安全服务需要涵盖河南省福利彩票发行中心(河南省养老事业发展中心)生产一机房、生产二机房、数据管理中心三个机房和生产系统（含电脑票热线销售系统和即开票销售系统）、计算机辅助管理系统（CAM）（含运营管理信息系统（OMIS）、办公自动化（OA）和渠道营销管理平台）、门户网站系统（河南福彩网）三个系统，并且具有可扩展性。

2）需要按照新的等级保护制度要求建设

按照《网络安全法》中明确了信息系统运营、使用单位应当按照网络安全等级保护制度要求，必须履行安全保护义务。并且随着新的等级保护制度的施行，等级保护 2.0 在原等级保护 1.0 的基础上，更加注重全方位主动防御、动态防御、整体防控和精准防护。福彩行业涉及广大彩民和重要数据信息，需要在新的等级保护制度要求下进行建设和完善。

3）需要制定适合福彩行业的安全建设方案

福彩业务所涉及的数据流、资金流和彩民信息都需要有严密的安全保障体系。本项目通过搭建平台和工具以提供安全服务时一定要根据行业的特点制定适合福彩行业的实施方案。福彩业务信息系统涉及面广、关注度高，信息安全服务既要符合国家有关法律法规的要求，也要满足中福彩中心信息安全要求。

4）需要实施不同区域的安全策略

根据等级保护制度的要求，首先对省中心网络和应用进行安全域划分，将业务外网和生产内网分开，并进一步细化为外部办公区、外联业务区、支撑业务区和核心业务区等，并根据不同的业务类型定义不同的安全策略。另外，对现有安全设备和安全策略进行优化和调整，并根据等级保护 2.0 的新要求补充新的安全工具、措施、服务手段等。

5）需要建立河南福彩行业整体防护体系

河南福彩行业整体防护体系一定要强调整体性，否则一个环节出现漏洞、出现短板，就会出现重大问题。等级保护 2.0 相对于过去，更强调立体的、多层次的主动防御能力和手段。这就需要建立从“被动防御”的思路到“主动防御”的思路，形成以防御为基础、以数据攻防分析为依据、以主动防御技术为武器，建立起福彩行业立体的、多层次的整体安全防护体系。

6）需要建立覆盖全省的运维管理平台

省中心各业务信息系统的网络结构复杂，既有电脑票、即开票等生产系统，也有渠道营销管理平台、OA、OMIS 等计算机辅助管理系统（CAM），还有银行、运营商、渠道商等外围系统和九千多个销售网点。从销售系统、辅助管理系统、外围系统、销售网点都可以到达中福彩中心和省中心，存在巨大的安全风险。另外，新的等级保护制度对人员和运维做了专门的明确要求，除了增加必要的人员以外，更需要建立起覆盖省中心的销售网点运维管理平台和服务工具，形成以“平台+工具+服务”为主体的运维管理体系。

7）需要建立专业团队进行网络及安全运维

等级保护 2.0 除了“技术要求”，还有相对应的“管理要求”，具体分为：安全管理制度、安全管理机构、安全人员管理、安全建设管理和安全运维管理等五个方面。网络及安全运维工作需要专业的信息安全技术人员，需要供应商建立一支既熟悉福彩行业又熟悉网络安全的专业团队派驻现场，配合省中心完成网络及安全运维工作。

（2）时间要求

序号	实施内容	时间要求	具体内容
1	需求分析	合同签订生效之日起 10 天内	根据等级保护要求、整改意见及河南福彩实际需求，提出安全实施方案，并交付采购人确认。
2	项目实施	合同签订生效之日起 30 天内	按照采购人确认的安全实施方案，制定出详细的实施细则，完成平台及工具的部署升级。
3	服务期限	不少于 365 天，具体服务周期以总预算除以单日服务费报价后取整位数确定	按照本项目的招标要求，服务期内提供安全服务。

（3）服务团队要求

中标供应商应根据项目需求为本项目配备专业服务团队，并满足以下具体要求：

1）★服务团队组成。供应商应就本项目配备一线驻场服务人员 3 人，其中 1 人为项目负责人，负

责项目整体协调管理、技术执行等工作。实际服务团队人员须与投标文件中承诺的人员一致，服务期内未经采购人同意不得擅自调换、减少人员。合同期内本项目驻场人员不得兼职其他工作。

2）团队人员能力要求。供应商为本项目配备的一线驻场人员、二线非驻场技术服务人员应当是中标供应商的技术骨干，熟悉河南福彩业务及相关政策，具有计算机相关证书或专业技术资格条件的可在评审因素中作为加分项予以考虑。

3）服务人员管理。中标供应商应严格遵守采购人单位相关管理规定，加强对服务人员的日常管理和考核。驻场服务人员应聚焦服务工作主责，驻场服务人员工作时间与采购人保持一致，节假日按照采购人实际要求进行。参与采购人重保 7*24 小时值班，值班结束离场时需办理相关手续后方可离场。严格遵守服务规范，文明服务，工作中遇到问题需及时向采购人反馈，不得与采购人发生争执。中标供应商应对配备的服务人员的人身安全负责。

（4）技术指标要求

1）销售网络基础安全防控服务

序号	名称		技术要求
1.	销售网络基础安全防控服务	主要服务内容	1、服务期内，利用销售网络基础安全防控服务平台提供“一站式”安全托管服务，所需的平台、工具和服务队伍由中标方提供，并满足新的等级保护制度（等级保护 2.0）建设要求、行业安全建设要求和定制开发。 2、销售网络安全服务平台包括但不局限于以下业务模块： ①态势感知平台（1 套，覆盖全网）； ②威胁情报联防平台（1 套，覆盖互联网入口）； ③销售网点运维管理平台（1 套，覆盖销售网点）； ★3、随着安全建设要求的不断提高，以及行业发展规模的不断扩大，在服务期内，供应商除提供现阶段“一站式”安全托管服务以外，销售网络基础安全防控服务平台及业务模块还需要根据实际情况不断补充和完善，以满足等级保护制度及行业的安全建设要求。 本项目不仅包括以上服务内容，而且还包括采购人由于信息系统变更、升级等衍生的新增服务内容（增量不超过以上服务内容的 10%），**供应商需要提供相关承诺函**。
2.	销售网络基础安全防控服务平台技术指标要求	态势感知平台	1、支持资产发现、漏洞扫描、安全事件采集、工单管理、多源日志关联分析、可视化大屏等功能。 2、支持采集的设备类型：路由器、交换机、防火墙、IDS/IPS、WAF 应用防火墙、APT 威胁检测防御设备、数据库审计、网络审计、堡垒机、主机监控系统、安全扫描设备、网页防篡改系统、Windows、Linux、Unix、Apache、IIS、JBoss、Tomcat、Nginx、WebLogic、牙木 DNS 等； 3、资产审核：支持资产的审核管理，与资产自动引擎识别等资产进行审核与信息不全，实现资产自动发现、资产审核以及资产入库管理的资产全生命周期管理； 4、支持事件的分类规则，可分为九大类、百余子类的事件分类，包括：网络安全事件、数据安全事件、业务安全事件、内容安全事件、主机安全事件、可用性安全事件、异常网络访问安全事件、合规性事件、系统运行事件。 5、支持对防火墙、SSL VPN、上网行为管理、数据库安全审计、入侵检测系统、入侵防御系

			统、Web 应用防火墙、防病毒网关、多网隔离安全网关、防火墙、运维安全审计系统（堡垒机）等设备进行集中管理，实现安全日志统一采集、审计和分析； 6、工单管理：支持漏洞、告警的派单处理，按照安全运维的设定流程进行工单流转并最终到达该告警的负责人，该负责人进行告警事件的处理，在处理过程中，该工作单的处理过程的各个状态可查看、可追踪。 7、支持大屏展示综合态势，从资产、漏洞、攻击、告警等维度呈现整体安全状态，包括安全评级、资产总数、漏洞分布、漏洞 top5、高危漏洞、告警总数、已封堵 ip、安全事件趋势等信息； 8、支持大屏展示资产态势，包括业务总数、资产总数、新增业务系统、新增风险业务系统、新增资产、新增风险资产、新增高危漏洞资产、资产应用 web 服务 top5、资产概况趋势、资产设备类型分布、开放服务排名等。 9、资产发现：内置资产自动发现引擎，支持与公安部一所、Webray、FOFA、知道创宇等第三方资产发现引擎联动，自动发现网络中的新资产，识别资产的 IP、URL、端口、服务、操作系统、安装的中间件、数据库等属性。 10、具备丰富的资产管理属性，支持通过资产名称、IP、域名、URL、所属单位、负责人、所属网络、所属业务、部署位置、等保定级、维护方等属性对资产进行标识和管理。 11、关联分析：支持针对日志或事件类型进行事件关联分析规则配置，并内置规则，包括：失陷主机活动、敏感数据传输、数据泄露、SQL 注入、提交 webshell 代码、违规访问敏感文件、代码执行攻击等； 12、支持响应方式，包括：邮件、微信等方式。支持将周期性日报、周报、月报通过微信推送到手机端。 13、提供丰富的报告模板，至少应包括：综合安全风险报告、外部威胁感知报告、脆弱性感知报告、综合处置报告、联动封堵审计报告。 14、支持对日志进行预处理，根据设备类型、源/目的 IP、源/目的端口、协议、日志分类状态码、地理位置、情报标签等内容选择指定日志进行预处理，灵活标记日志的准确度(1-10 级)、攻击工具类型、XFF 代理显示等;支持对需要留存的预处理规则进行启动、停止生效而不删除。 15、通报管理：支持将发现的攻击风险、漏洞风险及时通知给对应的人员，支持定义通报等级、受影响程度、紧急程度的不同定义，设计了发现节点、下发节点、修复节点、复查节点、审核节点、结束节点等流程，在不同的节点分配不同角色权限的员工进行处置。 ★16、行业对接：根据行业不同的业务类型定制建立不同的数据分析业务，如：电脑票游戏、即开游戏等，并符合行业对各类游戏的安全建设技术规范和对接要求。**供应商需要提供相关承诺函。** ★17、运行平台：≥2U 标准机架式设备，全模块化设计，标配 6 个千兆电口，4 个千兆 SFP 接口，3 个网络扩展槽，2 块 4T 硬盘，2 个 USB 接口，1 个 COM 口；配置 150 个监控节点授权；单电源；安全事件采集能力：3600 EPS；80 亿条日志存储能力。 ★18、**提供此平台的技术规格表**。

3.		威胁情报联防平台	1、阻断拦截：①支持串联与旁路部署情况下，检测出的同时对问题访问行为进行阻断拦截；②支持自动值守和人工研判的攻击阻断方式。 2、情报源支持：①系统支持接入正向攻击类情报源；系统支持接入 IP 画像溯源类情报；系统支持接入反向连接类情报源。②正向攻击类情报源更新频率不超过 2 分钟，反向连接类情报每天实时更新；③支持用户自定义私有情报源，获取方式为 FTP，更新频率支持自定义；正向攻击类情报，至少覆盖 30 个行业。 3、攻击检测：①系统支持在情报匹配的基础上，自定义开启对情报的二次本地校准；内置攻击监测策略以满足日常及重保等场景，并支持用户自定义攻击监测策略； ②支持针对不同资产分组设置特定的监控策略；③支持一键开启或关闭私有情报源；依托情报可根据不同安全防护等级设置情报碰撞策略，包含单个 IP 和 IP 所在 C 段；基于情报源、情报行业、情报类型、情报碰撞策略及情报威胁等级等维度有针对性的设置防护规则；具体匹配规则支持自定义匹配顺序。 4、外联检测：①支持针对不同资产分组设置特定的检测策略；②支持用户自定义外联域名库，可进行批量导入、导出、删除等操作；支持自定义外联检测范围，包括所有外联行为检测和命中情报外联行为检测。 5、弱口令登录检测：①支持自定义检测策略，可针对不同资产分组设置特定的检测策略；弱口令登录检测支持用户自定义检测字段；②支持用户自定义口令字典，可进行批量导入、导出、删除等操作。 6、溯源画像：IP 画像信息包含：归属地、运营商、资产信息及组件信息；溯源信息至少包含历史攻击时间、攻击目标、历史攻击单位、所属行业、攻击类型、威胁等级等信息，至少可溯源 5 条最近历史记录，以辅助研判。 7、统计分析：①针对攻击监测，支持攻击监测日志、攻击 IP 分析及被攻击 IP 分析等三个维度的统计，可通过丰富的组合筛选条件进行详细风险审计。②针对外联检测，支持外联检测日志、外联检测分析以及外联域名分析等三个维度的统计，可通过丰富的组合筛选条件进行详细审计；并支持情报及本地攻击行为的溯源。③支持整体攻击态势可视化展示，并可在地图上进行直观的情报 IP 分部查看，同时可直接在数据统计界面中进行人工研判。 ★8、联防联控：能够与公安部第一研究所等类似官方威胁情报中心实时联动，通过对全国各个行业提供的情报进行多源融合与智能分析，实现联防联控、情报共享，并做到“一点监控，全网阻断”。**供应商需要提供相关承诺函。** ★9、硬件平台：尺寸：≥1U 机架式；接口规格：1 个 console 口，2 个 USB 接口； 6 个千兆自适应电口，带 2 组 Bypass；带 2 个扩展槽；硬盘容量：1TB；电源规格：冗余电源；新建连接数：≥15000/秒；最大并发连接数：≥1000000；旁路阻断率：>80%；串联阻断率：>99%。
4.		销售网点运维管理平台	1、系统功能：负责全省销售网点安全接入终端设备的管理、维护、状态展示、报表生成。 2、终端设备管理：支持对销售网点安全接入终端设备的增、删、改及分域管理；支持单个及批量修改销售网点安全接入终端设备的配置；支持终端设备的启用、禁用。 3、终端设备运维：支持销售网点安全接入终端设备的远程登陆、故障排查；支持销售网点安全接入终端设备的远程升级；支持销售网点安全接入终端设备的维护信息录入、查询。 4、终端设备状态展示：支持销售网点安全接入终端设备的上网信息、在线信息、隧道信息等状态展示；支持销售网点安全接入终端设备的外网接入、销售终端接入、视频机接入、互联

			网使用等状态展示。 5、中心设备状态展示：支持展示中心设备的运行状态，包括 CPU、内存、硬盘等使用率；支持展示中心设备的网络状态，包括网络、服务、隧道等连接数；可自定义监控阈值，当状态异常时自动告警；可展示中心线路是否正常；中心线路异常时自动短信告警；可展示每条中心线路当前接入的终端数量。 6、大屏监控展示：支持在大屏上展示统一监控界面；支持大屏展示服务器监控状态、终端设备在线趋势图；支持大屏展示各类统计图表，包含在线图表、安装图表、地市统计图表等。 7、管理功能：支持设备使用报表的生成及导出；支持地市级管理员跨区域通过专用安全通道进行终端设备的运维管理；支持各种管理角色的定义与划分，支持管理员权限定制、管理内容定制。 ★8、销售终端的统一运维管理定制开发：安全接入终端是销售网点的核心接入设备，关联着销售终端、电子走势图、视频监控以及辅助销售设备，是销售网点的运维和管理重点，该系统需与现有的销售网点综合安全接入系统无缝兼容和联动，并实现全省数千个销售网点的安全接入终端、上万个各类销售设备、辅助销售设备等统一的系统监测、系统控制、系统管理，以及大屏展示定制开发。**本项目不仅包括以上服务内容，而且还包括采购人由于信息系统变更、升级等衍生的新增服务内容（增量不超过以上服务内容的 10%），供应商需要提供相关承诺函。** ★9、运行平台：提供的基于 ATCA 架构的物理板卡，支持热插拔，不低于 E5 系列六核双路 CPU，不小于 16G 内存，内置 2T 硬盘。至少 2 路 10GbE 网口、2 路 GbE 网口、2 个外置 GbE 电口。 ★10、提供此平台的技术规格表。
5.	销售网络基础安全防控服务平台定制开发	销售网点综合业务安全接入系统与平台的对接定制开发要求	1、销售网点与省中心、中福彩中心的网络相连，是福彩销售网络的末端，由于涉及范围大、涉及面广，是安全防控的重点，也是薄弱环节。服务期内，为了加强销售网点的综合安全防控能力，销售网络基础安全防控服务平台需要结合行业应用进行相关的对接和定制开发，包括但不局限于以下业务系统的对接和定制开发： ①态势感知平台； ②销售网点运维管理平台； 2、对接和定制开发的内容包括但不局限于以下模块： ①**态势感知平台定制开发：**需要建立实时监测销售网点与省中心的安全态势感知和日志审计管理中心，通过与销售网点“综合业务安全接入系统”进行无缝对接和联动，将销售网点安全接入终端、各类销售终端的日志进行收集和导入，建立起覆盖销售网点的安全态势感知系统。 ②**销售网点运维管理平台定制开发：**销售网点有全国统一的双色球、快乐 8，也有地方性游戏等，并且未来还有新游戏不断更新，各类终端根据不同游戏类型管理权和所有权各不相同。需要针对不同终端设备定制不同的运维管理策略，并与行业统一安全认证系统无缝对接和定制开发，实现行业性各类设备的安全认证、分级管理和系统运维要求。 3、供应商需提供运维管理系统《计算机软件著作权登记证书》以证明其开发能力。

2）核心业务区安全防控服务

序号	名称		技术要求
1	核心业务区安全防控服务	主要服务内容	1、服务期内，为核心业务区提供“一站式”安全托管服务，包括必要的安全设备、防护措施和安全服务，并满足最新的等级保护制度建设要求和行业安全建设要求。 2、核心业务区安全防控包括但不局限于以下业务系统防控： ①电脑票销售系统； ②即开票销售系统； ③辅助业务管理系统； ④综合安全接入系统； ★3、随着行业应用系统不断地增加，在服务期内，核心业务区业务系统及业务模块会不断变化，需要根据实际情况不断补充和完善，提供“一站式”安全解决方案，以满足等级保护制度及行业的安全建设要求。
2		主要防护措施	1、服务期内，利用销售网络基础安全防控服务平台为核心业务区提供基础安全防护服务，包括但不局限于以下业务模块： ①态势感知平台； ②威胁情报联防平台； ③销售网点运维管理平台； 2、服务期内，利用通用安全设备为核心业务区提供安全防护服务，包括但不局限于以下安全措施和安全设备： ①安全区域边界：实现访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计等安全措施； ②安全计算环境：实现入侵防范、恶意代码防范等安全措施； ③安全管理中心：实现集中管控等安全措施； ④部署安全设备：包括但不局限于防火墙、入侵防御、网络审计、数据库审计、WEB 应用防火墙、防病毒等； 3、服务期内，组建专业安全服务团队为核心业务区提供专业安全服务，包括但不局限于以下安全服务： ①安全评估渗透测试服务 ②定期巡检安全检查服务 ③紧急事件安全应急服务 ④重大事件安全值守服务 ⑤等级保护业务指导服务 ⑥专业团队驻场运维服务 ★4、以上设备具体数量、功能、性能和安全服务具体内容依据等保测评结果、整改意见、安全域划分以及行业应用要求提出建设方案进行完善和补充，并为核心业务区提供“一站式”防控服务，**本项目不仅包括以上服务内容，而且还包括采购人由于信息系统变更、升级等衍生的新增服务内容（增量不超过以上服务内容的 10%），供应商需要提供相关承诺函。**

3）辅助业务区安全防控服务

序号	名称		技术要求
1	辅助业务区安全防控服务	主要服务内容	1、服务期内，为支撑业务区提供“一站式”安全托管服务，包括必要的安全设备、防护措施和安全服务，并满足最新的等级保护制度建设要求和行业安全建设要求。 2、支撑业务区安全防控包括但不局限于以下接入管理： ①中福彩中心接入区； ②市福彩中心接入区； ③传统销售网点接入区； ④社会化网点接入区； ⑤便捷销售点接入区； ⑥彩票销售厅接入区； ★3、随着行业应用系统不断地增加，在服务期内，辅助业务区业务系统及业务模块会不断变化，需要根据实际情况不断补充完善，提供“一站式”安全解决方案，以满足等级保护制度及行业的安全建设要求。
2		主要防护措施	1、服务期内，利用销售网络基础安全防控服务平台为辅助业务区提供基础安全防护服务，包括但不局限于以下业务模块： ①态势感知平台； ②威胁情报联防平台； ③销售网点运维管理平台； 2、服务期内，利用通用安全设备为辅助业务区提供安全防护服务，包括但不局限于以下安全措施和安全设备： ①安全区域边界：实现访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计等安全措施； ②安全计算环境：实现入侵防范、恶意代码防范等安全措施； ③安全管理中心：实现集中管控等安全措施； ④部署安全设备：包括但不局限于防火墙、入侵防御、网络审计、数据库审计、WEB 应用防火墙、防病毒等； 3、服务期内，组建专业安全服务团队为支撑业务区提供专业安全服务，包括但不局限于以下安全服务： ①安全评估渗透测试服务 ②定期巡检安全检查服务 ③紧急事件安全应急服务 ④重大事件安全值守服务 ⑤等级保护业务指导服务 ⑥专业团队驻场运维服务..... ★4、以上设备具体数量、功能、性能和安全服务具体内容依据等保测评结果、整改意见、安全域划分以及行业应用要求提出建设方案进行完善和补充，并为辅助业务区提供“一站式”防控服务，**本项目不仅包括以上服务内容，而且还包括采购人由于信息系统变更、升级等衍**

			生的新增服务内容（增量不超过以上服务内容的 10%），供应商需要提供相关承诺函。

4）外联业务区安全防控服务

序号	名称		技术要求
1	外联业务区安全防控服务	主要服务内容	1、服务期内，为外联业务区提供“一站式”安全托管服务，包括必要的安全设备、防护措施和安全服务，并满足最新的等级保护制度建设要求和行业安全建设要求。 2、外联业务区安全防控包括但不局限于以下接入管理： ①联通、电信等运营商接入区； ②中行、邮储、农行等银行接入区； ③银联等金融及增值业务服务接入区； ④社会化网点运营等企业接入区； ★3、随着行业应用系统不断地增加，在服务期内，外联业务区业务系统及业务模块会不断变化，需要根据实际情况不断补充完善，提供“一站式”安全解决方案，以满足等级保护制度及行业的安全建设要求。
2		主要防护措施	1、服务期内，利用销售网络基础安全防控服务平台为外联业务区提供基础安全防护服务，包括但不局限于以下业务模块： ①态势感知平台； ②威胁情报联防平台； ③销售网点运维管理平台； 2、服务期内，利用通用安全设备为外联业务区提供安全防护服务，包括但不局限于以下安全措施和安全设备： ①安全区域边界：实现访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计等安全措施； ②安全计算环境：实现入侵防范、恶意代码防范等安全措施； ③安全管理中心：实现集中管控等安全措施； ④部署安全设备：包括但不局限于防火墙、入侵防御、网络审计、数据库审计、WEB 应用防火墙、防病毒等； 3、服务期内，组建专业安全服务团队为外联业务区提供专业安全服务，包括但不局限于以下安全服务： ①安全评估渗透测试服务 ②定期巡检安全检查服务 ③紧急事件安全应急服务 ④重大事件安全值守服务 ⑤等级保护业务指导服务 ⑥专业团队驻场运维服务..... ★4、以上设备具体数量、功能、性能和安全服务具体内容依据等保测评结果、整改意见、安

			全域划分以及行业应用要求提出建设方案进行完善和补充，并为外联业务区提供“一站式”防控服务，**本项目不仅包括以上服务内容，而且还包括采购人由于信息系统变更、升级等衍生的新增服务内容（增量不超过以上服务内容的 10%），供应商需要提供相关承诺函。**

5）外部办公区安全防控服务

序号	名称		技术要求
1	外部办公区安全防控服务	主要服务内容	1、服务期内，为外部办公区提供“一站式”安全托管服务，包括必要的安全设备、防护措施和安全服务，并满足最新的等级保护制度建设要求和行业安全建设要求。 2、服务期内，利用通用安全设备为外部办公区提供安全防护服务，包括但不局限于以下安全措施和安全设备： ①安全区域边界：实现访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计等安全措施； ②安全计算环境：实现入侵防范、恶意代码防范等安全措施； ③安全管理中心：实现集中管控等安全措施； ④部署安全设备：包括但不局限于防火墙、入侵防御、网络审计、数据库审计、WEB 应用防火墙、防病毒等； ★3、随着行业应用系统不断地增加，在服务期内，外部办公区业务系统及业务模块会不断变化，需要根据实际情况不断补充完善，提供“一站式”安全解决方案，以满足等级保护制度及行业的安全建设要求。
2		主要防护措施	1、服务期内，利用销售网络基础安全防控服务平台为外部办公区提供基础安全防护服务，包括但不局限于以下业务模块： ①态势感知平台； ②威胁情报联防平台； ③销售网点运维管理平台； 2、服务期内，利用通用安全设备为外部办公区提供安全防护服务，包括但不局限于以下安全措施和安全设备： ①安全区域边界：实现访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计等安全措施； ②安全计算环境：实现入侵防范、恶意代码防范等安全措施； ③安全管理中心：实现集中管控等安全措施； ④部署安全设备：包括但不局限于防火墙、入侵防御、网络审计、数据库审计、WEB 应用防火墙、防病毒等； 3、服务期内，组建专业安全服务团队为外部办公区提供专业安全服务，包括但不局限于以下安全服务： ①安全评估渗透测试服务 ②定期巡检安全检查服务 ③紧急事件安全应急服务 ④重大事件安全值守服务

			⑤等级保护业务指导服务 ⑥专业团队驻场运维服务..... ★4、以上设备具体数量、功能、性能和安全服务具体内容依据等保测评结果、整改意见、安全域划分以及行业应用要求提出建设方案进行完善和补充，并为外部办公区提供“一站式”防控服务，**本项目不仅包括以上服务内容，而且还包括采购人由于信息系统变更、升级等衍生的新增服务内容（增量不超过以上服务内容的 10%），供应商需要提供相关承诺函。**

6）销售网络安全加固服务

序号	名称		技术要求
1.	销售网络安全加固	主要服务内容	1、服务期内，利用网络安全工具进行加固服务，所需的软硬件系统、工具和服务队伍由供应商提供，并满足最新的等级保护制度建设要求和行业安全建设要求。 2、加固所需网络安全工具包括但不局限于以下内容： ①高级持续性威胁检测系统（2 台）； ②漏洞扫描系统（1 台）； ③防火墙（核心）（6 台）； ④防火墙（边界）（2 台）； ⑤防火墙（接入）（5 台）； ⑥入侵防御系统（2 台）； ⑦网络审计系统（3 台）； ⑧数据库审计系统（2 台）； ⑨日志审计（2 台）； ⑩WEB 应用防火墙（1）（2 台）； ⑪WEB 应用防火墙（2）（2 台）； ⑫WEB 应用防火墙（3）（2 台）； ⑬入侵检测系统（1 台）； ⑭堡垒机（2 台）； ⑮服务器防病毒系统（2 套，不少于 100 个服务器端）； ⑯终端防病毒系统（2 套，不少于 180 个 PC 端）； ⑰安全准入系统（1 台，不少于 180 个管理数）； ★3、随着安全建设要求的不断提高，以及行业发展规模的不断扩大，在服务期内，供应商除提供现阶段网络安全工具进行加固以外，还需要根据实际情况不断补充和完善，以满足等级保护制度及行业的安全建设要求。**本项目不仅包括以上服务内容，而且还包括采购人由于信息系统变更、升级等衍生的新增服务内容（增量不超过以上服务内容的 10%），供应商需要提供相关承诺函。**
2.	销售网络安全	高级持续性威	1、威胁检测：①支持对恶意软件利用、可疑行为、攻击利用、攻击探测、挖矿事件、APT 攻击事件等常见攻击类型进行检测。②支持自定义规则进行检测，自定义规则须支持工控协议，支持自定义检测规则的协议类型包括：TCP、UDP、ICMP, HTTP、SMTP、IMAP、POP3、MySQL、

	加固服务技术指标要求	胁检测系统	MSSQL、Oracle、MODBUS 等。自定义维度包括：事件名称、事件别名、事件说明、协议类型、事件级别、事件类型、影响系统、影响设备、IP 是否反转、攻击阶段、攻击状态、pcap 是否存储、自定义规则是否启用；可自定义的影响设备包括：LinuxOS、Windows OS、UNIX OS、多种操作系统、防火墙、交换及路由设备、网络带宽、多种网络设备；可自定义攻击阶段包括：发现（T1124）、侦查（T1597）、防御绕过（T1140）、执行（T1203）、命令控制（T1090）、凭证获取（T1056）、横向移动（T1210）、命令控制（T1092）、持久化（T1554）。具备数据包完整性检测、碎片重组检测、编码检测能力、高级逃逸 AET 检测等防逃逸检测能力。 2、威胁感知：①支持对当前监测网络整体安全态势进行整体感知，感知安全等级包括：高危、中危、低危、安全等。整体安全态势评估关键指标包括：失陷主机数、漏洞利用成功事件数、恶意样本投递事件数。②支持对攻击事件所处攻击阶段进行整体感知，可查看每个阶段攻击事件数，攻击阶段包括但不限于：侦查、发现、信息收集、初始访问、执行、特权提升、横向移动、命中与控制、持久化等。支持所监测网络内失陷主机进行整体感知，可通过监控界面点击跳转到事件处置界面进行失陷主机处置。支持跳转从两个出口中进行选择，跳转界面包括：僵木蠕攻击界面、恶意域名界面。 3、威胁分析：支持从不同视角对攻击事件进行威胁分析，专业视角不少于 6 个，专业视角包括：攻击者视角、被攻击者视角、事件视角、样本视角、恶意域名视角、威胁情报视角等。支持分析场景不少于 5 个，包括常见 WEB 攻击、僵木蠕攻击、扫描探测、暴力破解、可疑行为等进行智能场景化分析。WEB 攻击场景需支持查看攻击者 TOP、攻击结果、告警日志等信息，僵木蠕攻击场景需支持查看被攻击者 TOP、告警趋势、告警日志等信息。具备独立的研判界面，支持对告警事件进行研判分析，可查看告警事件的请求头、请求体、响应头、响应体或 payload, 并支持一键复制请求、响应信息；可下载告警事件的原始数据报文，提供在线报文分析；支持查看事件帮助信息，包括但不限于：事件名称、事件类型、协议类型、事件描述、CVE 编号、CNCVE 编号、事件性质判定、事件处理流程。 4、未知威胁检测：①未知威胁检测：支持输入解压密码对压缩文件进行检测，压缩文件解压深度至少支持 10 层解压，可选择对压缩文件是否进行解密。须内置沙箱，具备 100 种以上文件格式沙箱检测能力，支持自定义文件类型，支持检测的协议类型包括：SMTP、IMAP. FTP、POP3、SMB、HTTP、HTTPS 等。支持检测：打开系统进程中的线程、启动可疑进程、启动子进程、向系统进程内写入数据、注入其他进程、在系统进程中创建远程线程、遍历进程、向其他进程写入可疑内容等敏感行为；②支持记录：进程启动等详细行为信息。样本报告能够显示进程/线程状态、注册表项操作、文件操作、互斥量操作、网络操作、服务相关、关键 API 调用等行为等信息供分析。 ★5、运行平台：≥2U 上架设备，提供 2 个 1000M Base-T 网络接口，2 个 10/100/1000M Base-T 网络接口，最多提供 7 个扩展槽位，冗余电源，32T 容量硬盘。
3.		漏洞扫描系统	1、系统要求：①提供对 Web 应用的 SQL 注入漏洞、命令注入、CRLF 注入、LDAP 注入、XSS 跨站脚本漏洞、路径遍历漏洞、信息泄漏漏洞、URL 跳转漏洞、文件包含漏洞、应用程序漏洞、文件上传漏洞、struts2 命令执行等进行检测。提供针对已发现的 Web 应用的漏洞进行验证。②支持漏洞验证功能，在扫描结束后，能够对结果中的重要漏洞进行现场验证，展示漏洞利用过程和风险。支持自定义 HTTP 版本、链接超时时间、数据发送超时时间、数据接收超时时间、链接超时重试次数和 http 请求头，支持自定义扫描策略模板和模板管理，支

			持策略模板导入导出。 2、后台管理要求：①支持按照选择的用户来筛选如下任务：检测任务，监控任务，变更任务，DNS 任务、告警任务；②支持按照用户或者部门来选定时间段下载报表。支持授权文件上传、在线升级、离线升级方式；③支持登录配置、新闻配置、邮件服务器配置、系统网卡设置、引擎设置、DNS 服务器配置等。 3、网站监控：①支持网站可用性和网站详情监控，Ping、HTTP、GET 请求等网站安全监控功能。支持基于网站连接通断的可用性监控和基于响应时间的性能监控；②支持当前网页和快照的文件和图片对比，不同的文本区域应使用不同颜色标出；支持配置多个 DNS 服务器，对各 DNS 服务器的解析结果进行对比；③支持对解析到的异常 DNS 地址进行邮件报警；④支持关键字检测功能，并能自定义关键字。 ★4、运行平台：便携笔记本形态，标配 1 个 10/100/1000M 网口，2 个 USB 接口，单交流电源）一台；系统漏扫授权，不限制扫描的 IP 地址，并发扫描 20IP； Web 应用检测模块使用授权，可扫描域名地址总数量为 256 个；安全基线配置核查管理模块，默认包含安全基线配置核查管理系统中的标准功能模块，提供 Windows 系列（Win2003、win2008、winXP、win7）安全配置核查，并发 20 资产扫描。安全基线配置核查管理模块资产数量授权，扫描范围不限制，限制在创建作业时能添加的资产数量总数为 256 个，限制作业合并后导出报告中包含的资产总数为 256 个。
4.		防火墙（核心）	1、系统要求：具有防火墙（IPV、AV）的基本功能。需支持多系统引导，并可配置启动顺序，多系统设置可在 Web 界面上完成全部操作。 2、入侵防护：支持 IPv4 和 IPv6 双栈协议下的入侵检测与防护；内置 IPS 特征库，并可自定义入侵攻击和应用软件的特征；入侵防御事件库至少应包括木马后门、间谍软件、可疑行为、安全漏洞及网络数据库攻击等的特征事件；支持端口扫描和主机扫描防护。 3、病毒防护：①支持 IPv4 和 IPv6 双栈协议下的病毒扫描与防护；支持 HTTP，SMTP，FTP，PO3P，IMAP 等多种应用协议下病毒防护，支持自定义非标准端口下应用协议的病毒防护；②支持多接口可旁路的病毒文件传输监听检测方式，可并行监听并检测多个网段内的病毒传输行为，用于高可靠性要求的旁路应用环境；支持病毒感染主机分析与隔离，防止病毒进一步扩散，提高网络整体安全性。 ★4、≥2U 机架式设备，配置冗余双电源，电口支持硬件 BYPASS；标配 6 个 10/100/1000M Base-TX,1 个 Console 口，2 个 USB 口,4 个扩展槽位，最大支持扩展千兆网络接口 38 个；整机吞吐不小于 10Gbps，每秒新建连接数不小于 8 万，并发连接数不小于 320 万。
5.		防火墙（边界）	1、系统要求：具有防火墙（IPV、AV）的基本功能。需支持多系统引导，并可配置启动顺序，多系统设置可在 Web 界面上完成全部操作。 2、入侵防护：支持 IPv4 和 IPv6 双栈协议下的入侵检测与防护；内置 IPS 特征库，并可自定义入侵攻击和应用软件的特征；入侵防御事件库至少应包括木马后门、间谍软件、可疑行为、安全漏洞及网络数据库攻击等的特征事件；支持端口扫描和主机扫描防护。 3、病毒防护：①支持 IPv4 和 IPv6 双栈协议下的病毒扫描与防护；支持 HTTP，SMTP，FTP，PO3P，IMAP 等多种应用协议下病毒防护，支持自定义非标准端口下应用协议的病毒防护；②支持多接口可旁路的病毒文件传输监听检测方式，可并行监听并检测多个网段内的病毒传输行为，用于高可靠性要求的旁路应用环境；③支持病毒感染主机分析与隔离，防止病毒进一

			步扩散，提高网络整体安全性。 ★4、≥1U 机架式设备，电口支持硬件 BYPASS；标配 2 个 10/100MBase-TX，4 个 10/100/1000MBase-TX；1 个 Console 口，2 个 USB 口；1 个扩展槽位，最大支持扩展千兆网络接口 8 个；整机吞吐不小于 2Gbps，每秒新建连接数不小于 1.2 万，并发连接数不小于 180 万。
6.		防火墙（接入）	1、提供虚拟路由器与虚拟交换机；提供 BFD 检测；提供 OSPF、BGP、ISIS（路由协议非透传）、提供基于时间与应用的策略路由，并可以与监测对象关联（TCP /HTTP/DNS 等），监测对象失败时，策略路由失效； 2、具备对勒索，木马等病毒文件的检测管控，支持自定义 IP 黑名单的容量，支持具备 Mac 地址的黑名单管控能力； 3、支持按功能模块统计丢包数量，包括但不限于策略、会话、UDP 等模块的丢包五元组统计，支持丢包趋势、实时丢包 Top10 展示，支持查看至少 180 天内的监控数据，支持以最近一小时、最近一天、最近一周、自定义时间筛选方式展示统计数据； 4、支持故障场景排查功能，支持模拟检测场景、在线检测场景、数据包导入检测场景，检测完成后，支持查看检测报告，协助管理员快速定位问题； 5、提供策略优化与策略助手功能；策略优化可对当前策略进行多维度分析，包括策略创建时间、首次命中时间、最近一次命中时间、最近未命中天数等；策略助手支持关联策略 ID 进行获取流量，并支持策略聚合条件，可一键生成策略，满足新业务上线策略梳理要求； 6、具备扩展云端沙箱功能，当设备本身无法判定是否是未知威胁时，由云沙箱引擎提交给云沙箱进行未知威胁检测，返回检测结果，并呈现云沙箱检测未知威胁的完整证据链; 7、零信任功能：提供零信任网络接入功能，设备支持 SPA 功能，拥有独立的零信任策略配置界面，可基于用户身份、终端标签和应用资源进行安全管控；拥有独立的终端标签日志界面，支持展示用户名、IP、终端 IP、操作系统等；提供不少于 8 个零信任接入授权； 8、提供应用识别，入侵防御，病毒过滤，威胁情报功能； ★9、≥1U 机架式设备，采用前后通风设计；产品具备≥8 个千兆电口，≥8 个千兆光口，≥2 个万兆光口；≥1 个 MGT 接口；支持扩展双冗余电源；防火墙吞吐量≥16Gbps，最大并发连接数≥400 万，每秒新建连接数≥13 万；标配 IPSEC VPN 6000 条免费隧道授权，标配 8 个免费 SSL VPN 用户授权，SSL VPN 并发用户数最大支持扩展到 4000 个。
7.		入侵防御系统	1、入侵防御功能：①系统可检测的入侵防御事件库事件数量不少于 4000 条，系统应支持事件响应模版，能够批量修改事件响应动作，包括：事件级别、事件启用开关、动作、日志合并方式、日志开关、抓包取证。②系统应支持弱口令检测功能，需支持至少 8 种网络协议并支持至少 7 种弱口令检测元素，文字说明支持的网络协议和定义弱口令的检测元素。③系统应支持多种防 web 扫描能力，包括爬虫、CGI 和漏洞扫描等，并支持设置至少 4 个不同级别的扫描容忍度/扫描敏感度。 2、病毒防御功能：①系统应支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于 50 万。②系统应支持 HTTP 协议和邮件协议防病毒，通过信息替换功能，用以通知用户病毒被阻断，管理员可以自行设置替换信息。③为保证病毒检测的可靠性，要求系统应至少支持双病毒引擎。 3、恶意代码检测功能：①系统应提供扩展静态恶意代码（APT）检测引擎，针对 HTTP、FTP、SMTP 等协议中包含的未知恶意文件进行检测。②系统应支持可扩展恶意样本自学习功能，除

			通过网络文件捕获外，还支持通过系统直接上传文件，自动识别黑白文件并提供简要信息。 系统应支持可扩展未知 C&C 通道（隐蔽通道）检测功能，能够提供 C&C 通道的危险级别、连接建立时间、连接持续时间、控制端 IP 地址和端口、受控端 IP 地址和端口等 C&C 通道信息。 ③系统除具备可扩展的本地恶意代码检测功能外，还应具备云查杀、云检测等防御机制。 ★4、≥2U 硬件平台，配置冗余双电源，电口支持硬件 BYPASS；1 个带外管理口，1 个 HA 口，4 个接口扩展插槽，扩展 4GE、4SFP 业务接口；最大支持 16 路千兆电口或 16 路千兆光口或 4 路万兆光口；最大吞吐量 18G，最大并发 300 万，IPS 吞吐量 5G。
8.		网络审计系统	1、部署管理：支持旁路部署方式对原有网络不造成影响，网络审计自身的故障不影响被审计系统的正常运行；支持透明部署、支持 Bypass；可 HA 部署，支持主备方式；支持对部署在 vmware、KVM、Xen 等虚拟化环境中的数据库进行审计，审计系统可虚拟化部署。 2、审计能力：①支持对网盘文件传输的审计，可记录百度网盘、360 云盘等传输的文件名、文件大小、IP 地址、MAC 地址、传输时间等信息；②支持对常用网络游戏、股票软件、IM 软件、P2P 软件、流媒体的审计；支持与恶意 URL 的检测，可以对不良站点访问的详细记录；③审计策略支持时间、源 IP、目的 IP、协议、端口、登陆账号、命令作为响应条件。 3、审计协议：支持对 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache、MongoDB、Redis、Hbase、hive 等数据库进行审计；支持人大金仓 KingBase、神通(OSCAR)、达梦(DM)、南大通用(GBase)；支持 FTP、Rlogin、Radius、NFS、X11 等协议审计；支持 RDP 协议审计，可审计关键的键盘输入，记录会话过程；支持对邮件协议的审计，包括 pop3、smtp 及 Imap 等。 4、统计模版：系统应内置统计分析模板，统计模板包括且不限于：趋势分析、统计分析、性能分析等，且支持自定义模板，自定义条件包括源 IP、目的 IP、资源账号、客户端名称、协议等 10 几种。 ★5、≥1U 机架式设备；标配 6 个千兆电口，1 个千兆带外管理口，1 个千兆 HA 口，1 个 RJ45 串口，2 个 USB 口；1 个扩展槽位，最大可扩展至 10 个千兆电口；1 个 CF 卡插槽，存储容量 2T，内存 8G；可审计流量不小于 140Mbps，入库速度不小于 6000 条/秒，日处理事件数不小于 8000 万条。
9.		数据库审计系统	1、审计范围：支持对 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache、MongoDB、Redis 数据库进行审计；支持对人大金仓、达梦、南大通用数据库的审计。 2、审计功能：支持网络邻居、NFS 协议、Radius 协议审计；支持对针对数据库的 XSS、SQL 攻击行为进行审计；提供对数据库返回码的知识库和实时说明；支持数据库并发会话数、并发进程数、并发用户数、并发游标数、并发事务数、数据库锁等超过限制的审计 。 3、审计能力：针对异常场景自动生成审计结果，异常场景包含且不限于异常账号访问审计、数据库异常审计、同账号多 IP 登陆、同账号上下班时间操作统计、访问时长异常审计、操作全审计等；支持对于短时间内相同账号多个 IP 地址登陆的自动发现与审计，用以发现账号被盗用等异常；支持对相同账号下班时间操作多于上班时间的异常操作自动发现和审计。 4、系统管理：提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能；审计系统上存在大量敏感信息，必须对审计管理员进行强度更高的认证，管理员登陆支持硬件令牌认证；提供磁

			盘存储容量不足、磁盘 Raid 故障等自动邮件报警；提供 CPU、内存、磁盘、网口、运行时间、运行状态等信息的监视功能；提供审计策略和配置的导入导出。 ★5、≥1U 机架式设备；业务接口数量：不少于 6 个千兆电口，最大支持 12 个业务口；最少支持 1 个接口扩展槽；1 个 RJ45 串口、2 个 USB 接口；可用存储空间 2T,内存 8G;1 个 CF 卡插槽；可审计流量不少于 140Mbps；每秒入库速度不小于 6000；日处理事件数不少于 80000 万条。
10.		日志审计	1、设备监控要求：支持各类型日志磁盘存储占比统计、各类型日志接收趋势统计、设备日志接收趋势统计、发送日志的设备状态监控、硬盘健康状态及 Raid 状态监控； 2、NAT 日志审计：可记录详细 NAT 日志信息（包括时间、源地址、目的地址、端口以及转换后地址等元素），用户可以根据上述信息元素对安全审计平台收集的 NAT 日志进行检索查询； 3、系统日志：包括事件日志、告警日志、网络日志、配置日志、安全威胁日志等。内容审计日志：包括发帖日志、EMAL 日志、FTP 等日志； 4、URL 日志审计：可详细地记录 URL 日志信息（包括时间、源地址、目的地址、源端口、目的端口、以及 NAT 转换后地址、端口、URL 地址、用户等信息），可以收集、存储上述 URL 日志并提供快速的搜索查询功能； 5、IM 上下线审计：可以对 IM 上下线（包括移动 QQ）日志进行详细的记录（包括时间、内网地址、端口、NAT 后的地址和端口、IM 类型等信息）可以对上述信息进行采集、存储并提供快速检索查询的功能；； 6、日志备份：提供了日志备份的功能。针对客户海量的 NAT 日志、URL 日志和 IM 上下线日志，可以通过手动或者自动两种方式，把日志备份到第三方的存储空间，保证了日志数据的完整性； 7、支持二进制日志，支持同品牌防火墙进行二进制日志传输，压缩存储空间，提高日志存储效率；二进制日志包括 URL 日志、IM 日志、NAT 日志、SLB 日志、NAT444 日志等； 8、支持各类型日志磁盘存储占比统计和各类型日志接收趋势统计；支持各设备日志接收趋势统计；支持对发送日志的设备状态监控，支持硬盘健康状态及 Raid 状态监控，支持自定义监控面板和监控内容； 9、功能开发与漏洞修复：可根据安全需求开发新功能和修复产品漏洞； 10、≥1U 机架式设备，专用硬件安全审计设备，非通用 WINDOWS 平台；标配≥6 个千兆电口，≥1 个接口扩展槽；双电源，存储容量：4TB；日志处理速度：18,000 事件/秒；提供 100 个日志源授权。
11.		WEB 应用防火墙（1）	1、应用防护：支持对 HTTP、HTTPS 加密数据流进行分析保护；支持对 HTTP0.9、HTTP1.0、HTTP1.1、HTTP2.0 和 WebSocket 协议的安全防护；能够针对 SQL 注入、跨站脚本、目录泄漏、目录遍历、Cookie 假冒、认证逃避、命令行注入、HTTP 协议规范等攻击行为进行检查和阻断。 2、应用控制：提供基于 URL 级别的时域控制，能根据访问者的 IP/地域、访问目标 URL、时间等条件进行访问控制；支持应用和 URL 级别每秒请求数、每秒新建连接数、连接总数、请求总数控制；支持 CC 攻击防范和缓解；支持基于规则多维度(时间、路径、应用等几十项维度)多层次的自定义 CC 防护。 3、行为审计：能够对攻击来源、数据、时间、处理结果形成列表，提供多种基于行为的审计报表；能够对用户使用的客户端进行分析，了解用户访问应用系统使用的客户端情况；文件

			上传/下载审计，能够记录通过 HTTP 进行的文件上传/下载行为。 ★4、≥2U 机架式设备，不少于 4*1000BASE-T，2*SFP，1*RS232，可根据需求进行扩展。HTTP 请求/秒:不低于 25,000，TCP 并发连接: 不低于 2,500,000；单接口吞吐量(Mbps):不低于 1000M，整机吞吐量(Gbps):不低于 4G。
12.		WEB 应用防火墙（2）	1、支持通过 BGP 方式对流量进行牵引，并在清洗攻击后回注，回注过程支持设置 SNAT 策略。 2、支持 HTTP 访问控制，可根据实际网络状况自定义请求方法等参数的访问控制规则，过滤非法请求。 3、应能识别和阻断注入攻击，支持防扫描陷阱、爬虫防护，支持文件上传、下载过滤。 4、支持 IDP 防御功能，并提供 IDP 防御特征库，特征库需要提供 10 种类型并提供至少 10000 条 IDP 特征库；支持 IDP 防御策略设置，支持防护等级、处理动作，特征库等多项策略选择。 5、支持通过移动终端管理，不需要安装 APP 和第三方插件，通过手机浏览器即可,并可管理设备实现网站快速应急处置； 6、对网页请求/响应内容中的非法关键字进行检测、过滤，识别和防止敏感信息泄露，支持弱密码保护功能； 7、支持通过自学习的 URL 参数的长度、类型、范围及请求方法等数据特点创建黑白名单模型，如果参数违反模型则判断为非法流量，直接执行阻断或封禁动作。 8、支持第三方威胁情报库更新，支持利用威胁情报规则进行防护，可基于威胁情报的日志查询。 9、支持网站自学习建模，可通过学习 URL、host 等信息展示网站结构树形图，并支持对 URL 的访问量和响应健康度进行图形化统计。 10、支持 HTTP 协议校验，可根据实际网络状况自定义协议参数合规标准，过滤非法数据。 11、支持丰富的 WEB 防护功能，能够对 web 源代码进行扫描，检查代码中的网页木马，网页挂马以及网页暗链，并支持自定义规则。 ★12、≥1U 标准机架，标准配置 6 个千兆电口、1 个扩展槽；整机最大可支持 10 个千兆接口；2 个 USB，1 个控制口，1T 硬盘。HTTP 吞吐：200Mbps；HTTP 新建连接（CPS）：2000/s；HTTP 最大并发连接：30 万；WEB 防护：8 个站点；DDOS 防护：50 个站点；防篡改：2 个节点。
13.		WEB 应用防火墙（3）	1、注入防护：支持对 SQL 注入、LDAP 注入、SSI 指令注入、Xpath 注入、命令注入、邮件注入、远程文件包含、本地文件包含以及其他注入进行防御； 2、数据防泄露：支持个人敏感信息防泄漏功能，检测到个人身份信息（包括手机号、中国大陆、港澳台身份证号）、银行卡号、信用卡号、邮件账号的信息泄露； 3、访问控制：根据客户端 IP、HTTP 操作方法、HTTP 头名称、HTTP 内容类型、HTTP 协议版本、URI 路径等进行访问控制，支持 Host、 User-Agent、Accept、Accept-Language、Accept-Encoding、Referer、Cookie 等 HTTP 头部的策略控制； 4、支持对保护站点的流量进行智能学习，并根据学习结果生成针对性的防护策略；学习的内容包括：学习中、学习完成及学习到的 URL 地址、HTTP 请求个数、HTTP 访问方法等信息； 5、系统内置 Web 应用漏扫，包括：SQL 注入漏洞、XSS 攻击漏洞、Web 服务漏洞、信息泄露漏洞、异常访问漏洞；对 URL 扫描深度、链接总数、表单填充进行限制，根据扫描报告生成虚拟补丁； 6、提供 SaaS 运维平台，支持将设备信息、数据流量、威胁事件、系统日志等在云端提供可

			视化展示，通过手机 APP 方式进行远程监控设备状态信息、获取报表、威胁分析等； 7、提供手机 APP“一键断网”功能，被断网的网站自动跳转至自定义“维护中”页面，以满足监管部门限时断网的要求； 8、提供 API 防护策略，支持导入 OpenAPI 文件，文件格式支持.json、.yaml、.yml 等，支持根据 Host、URI 路径、HTTP 方法、HTTP 头部内容、请求行参数、请求体等内容设置自定义防护类型； 9、支持以客户端 IP、X-header 地址、TCP option 地址、服务器 IP、域名、规则 ID、URL、漏洞 ID 等字段进行 WEB 安全日志的查询与过滤，支持以客户端 IP 和防护类型进行日志的聚合查询； 10、支持 WEB 应用安全监控大屏展示，以大屏形势直观展示攻击地理威胁分布、热点威胁事件、风险站点排名、站点性能信息等； ★11、标配 16 个 GE 电口（含 2 组 bypass），8 个千兆光口，2 个万兆光口；标配 480G SSD 存储空间，单电源，支持扩展双冗余电源；网络层吞吐≥13Gbps，应用层吞吐≥8Gbps，最大并发连接数≥75 万，防护站点≥32 个。
14.		入侵检测系统	1、展示选定时间内的攻击趋势、攻击总数、攻击源 IP Top10、攻击目的 IP Top10、攻击协议统计、攻击严重性统计、攻击类型统计、攻击详情； 2、展示选定时间内的文件检测威胁趋势、危险文件总数、危险文件下载源 IP Top10、危险文件下载目标 IP Top10、病毒文件类型、文件关联邮箱、文件关联 URL、文件报告列表，提供病毒文件样本下载功能； 3、展示选定时间内的扫描探测趋势、扫描探测总数、扫描探测源 IP Top10、扫描探测目的 IP Top10、扫描探测详细信息； 4、以全球、中国两个维度，滚动展示今天、昨天、最近 7 天和最近 30 天的热点攻击； 5、统计和展示高可疑近 1 小时、8 小时、12 小时、1 天、7 天和 30 天内的告警 Top5、中可以告警 Top5 和低可疑告警 Top5; 5、监控和展示系统当前的固态硬盘、机械硬盘使用情况、健康状态；监控和展示系统各个网络接口的收发包流量和网络连线情况； 7、事件详情查看中以分类规整方式动态嵌入与之相关的攻击证据，并能实现证据内容的无限次数的钻取。分类方式应包括：尝试获取用户信息、疑似敏感行为、尝试获取用户权限、疑似 Web 应用攻击、疑似木马活动、病毒扫描、协议异常、网络扫描、异常连接； 8、展示选定时间内的恶意外联趋势、恶意外联总数、恶意外联活跃域名统计 Top10、恶意外联源 IP Top10、恶意外联关系图、恶意外联类型、恶意外联详细信息； 9、展示选定时间内的 Web 攻击趋势、Web 攻击总数、Web 攻击源 IP Top10、Web 攻击目的 IP Top10、Web 攻击 URL 统计、Web 攻击返回码统计、Web 攻击类型统计、Web 攻击详情； 10、当服务器前端部署代理设备或 CDN 时，通过配置源 IP 解析规则，获取真实的攻击源 IP 地址，支持配置规则名称、解析方法、解析字段、代理级数、规则状态等信息； ★11、≥1U 标准机架，标准配置 6 个千兆电口、1 个扩展槽；2 个 USB、1 个控制口；128G SSD、1T 硬盘。网络吞吐：1.5Gbps，IPS 吞吐：300Mbps，新建连接：1 万，并发连接：80 万。

15.		堡垒机	1、字符型远程操作协议：SSH(V1、V2)、TELNET、RLOGIN、AS400、图形化远程操作协议 RDP、VNC、X11；文件传输协议：FTP、SFTP； 数据库远程操作协议：支持 ORACLE、MSSQL、Sybase、Mysql、DB2、Postgresql 数据库远程访问协议审计； 2、支持通过应用发布的代理进行协议扩展，支持 Radmin、Pcanywhere、 HTTP/HTTPS，可自定义其它访问协议及客户端支持，具备应用发布方式访问 web 资源越权访问提示及阻断功能； 3、支持按用户(用户组)、目标设备(设备组)、系统帐号、命令集和生效时间内容设置访问授权策略可对违规操作、高危操作、访问异常内容设定安全事件的告警规则；支持 FTP/SFTP、RDP 剪切板支持上传、下载单独进行传输控制；支持添加对字符命令和数据库命令的指令集合的策略，策略的响应动作包括指令审批、忽略指令、阻断会话、产生告警； 4、支持全局开启安全运维模式，开启后仅能使用 web 客户端进行运维，且 web 客户端存在水印；支持全局开启菜单列表模式，菜单模式选择设备时不再需要层级选择，可以一次选中所需连接的设备账号和协议； 5、Web 访问方式：H5 运维支持现版本中所有远程协议，运维操作无需 JAVA 支持和客户端； 通过 Web 页面直接访问服务器或通过 Web 页面调用本地工具（含数据库客户端）直接访问服务器； 6、支持多种认证方式：本地密码认证、UsbKey 认证、TOTP 令牌认证(google 身份验证小程序验证)、第三方 CA 证书认证、指纹认证、邮件认证、RADIUS 认证、LDAP 认证、AD 域认证以及短信认证(支持阿里云、电信等短信网关)，支持应用发布方式访问 WEB 资源越权访问提示及阻断功能； 7、访问授权：支持对重要字符命令和数据库命令进行实时审核，运维人员执行命令后，系统响应动作包括，指令审批、忽略指令、阻断会话、产生告警；支持的数据库命令包括 ORACLE、MSSQL、Sybase、Mysql、DB2、Postgresql 等数据库； 8、访问控制及异常告警：支持客户端检测账号异常、ip 变化等因素，启用后用户的 ip 地址发生变更将无法继续访问堡垒机，并进行告警，支持限定访问 API 接口的 IP 地址设置； 9、支持自动改密策略，支持按计划执行时间、改密周期、密码策略、改密结果发送生成详细的改密计划，到期自动执行；支持自动发现主机，可设定检测网段和服务端口进行扫描，支持对已添加特权账号的设备进行账号稽查，并纳管未托管账号； 10、≥1U 机架式设备，配备千兆电口≥6 个、接口扩展槽≥1 个，支持扩展万兆接口，内置系统硬盘≥128G MSATA、内置数据硬盘≥4T，内存≥8G，字符并发≥100、图形并发≥90、mysql 并发≥100，双电源；提供≥150 个运维点数授权。
16.		服务器防病毒系统	1、基本要求：支持 Windows 类、 Linux 类服务器环境，支持信创服务器环境，支持与现用防病毒系统平滑升级，控制中心统一管控，客户端无需任何操作，提升管理方便性，不少于 100 个客户端授权，服务期内升级服务。 2、系统安全性：支持各功能组件间通过网络传输的数据进行保护，防止被非授权获取。 3、客户端占用：Windows 环境静默状态下客户端占用服务器内存不超过 20MB，CPU 单核使用率不超过 5%；工作状态状态下客户端 Agent 占用服务器内存不超过 20MB，CPU 单核使用率不超过 5%。Linux 环境静默状态下客户端占用服务器内存不超过 100MB，CPU 单核使用率不超过 5%；工作状态下的内存不超过 150MB，CPU 单核使用率不超过 5%。 4、勒索病毒防护：具备勒索病毒场景化防护能力，可在同一界面进行暴露面收敛、远程访问

			控制、系统风险点排查、勒索加固防护、勒索病毒实时查杀、勒索病毒应急处置等操作；内置勒索病毒防护策略模版，可通过一键策略下发的方式进行策略配置，降低运维难度。 5、资产检测：支持以列表的形式，统一列出 Windows/Linux 服务器基础信息，并在列表中对服务器的关键软硬件进行统计，包括但不限于：CPU 数、CPU 核数、分区数、账户数、软件应用数、web 站点数、web 服务数、web 框架数、数据库数、端口数、网络连接数、启动服务数、安装包数、计划任务数、环境变量数、内核模块数、证书数、注册表数、类库数等； 6、病毒防护：支持病毒实时防护功能，提供自主研发的病毒引擎，支持通过连接互联网，利用最新的病毒库进行病毒扫描和查杀；支持例外设置功能，包括文件例外设置以及后缀例外设置：文件例外需支持文件和目录路径例外设置、后缀例外需支持匹配文件扩展名的设置； 支持对压缩包文件进行监控，监控不少于 10 层压缩包文件；支持对 Linux 和 Windows 系统下的压缩包文件类型进行扫描:支持针对病毒扫描支持对扫描文件大小、系统资源进行设置，提供业务优先模式；支持对服务器的软件漏洞进行综合扫描，并可对扫描方式、扫描周期进行设置；支持对扫描出的软件漏洞进行标记修复、加白、应用虚拟补丁等操作，并支持漏洞复扫，支持对发现的漏洞进行“虚拟补丁”处置，防止漏洞被利用。 7、威胁监测：具备检测并阻断系统内存密码盗窃行为，防止攻击者通过该手段进行恶意登陆并进行攻击。具备阻止攻击者在系统可执行文件中任意添加恶意代码的能力，可检测并阻断攻击者更改系统可执行文件行为。 8、系统防护：支持防端口扫描功能，且可设置单个 IP 请求时间范围、最大扫描端口数量、IP 锁定事件等信息； 支持对服务器中复用的相同密码进行检测，可识别出某个密码被哪些服务器、哪个账户、在什么操作系统上进行了复用；支持对多个主机采用同一口令的密码复用情况进行检测，支持对复用密码的显隐、导出、删除。
17.		终端防病毒系统	1、基本要求：支持现用防病毒系统平滑升级，采用 B/S、C/S 混合架构，支持级联部署、单一部署、集群、虚拟机部署，不少于 180 个客户端授权，服务期内特征库升级服务。支持统一管理 WINDOWS 类、LINUX 类、macOS 类、国产化类（包括但不限于中标麒麟、银河麒麟、麒麟、统信等）。 2、安全管理：支持按 IP 地址、CPU 数量、MEM 容量、主机名、计算机工作组等参数进行自动动态调整分组，可以根据分组、计算机名称、IP 地址、操作系统、在线状态等条件的组合筛选出符合条件的终端进行管理。持自动分组，可以按 IP 地址、CPU 数量、MEM 容量、主机名、计算机工作组等参数进行自动动态调整分组。 支持客户端连接控制中心下载文件限速和日志上传限速，可设置带宽最大使量和限速时间，避免过多占用网络带宽，影响业务办公。 具备防退出密码保护、防卸载密码保护、防安装密码保护，具有自我保护能力，有效防止客户端进程被恶意终止、注入，提高客户端进程、数据、配置的安全性。 支持单个页面展示终端部署统计、终端安全趋势、终端状态（文件防护开启率、终端病毒更新率和终端版本更新率）、终端程序版本、终端在线统计、病毒库版本分布等信息，均可通过图形化展示。 支持控制中心登录账号输入密码错误次数超过自定义的锁定阈值后账号将被锁定，支持双因子认证登录方式。

			支持查看终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本 支持病毒查杀趋势、扫描触发方式趋势、发现病毒趋势、终端感染趋势、病毒类型统计、病毒处理结果统计、病毒发现触、方式统计、趋势图表、按分组、按终端、按病毒名称等病毒报表 3、病毒防护：支持信任区设置，病毒扫描或实时防护时不扫描目录或文件。 支持对进程防护、注册表防护、驱动防护、U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护、勒索软件防护。 支持扫描时资源占用限制，可设置如不限制、均衡、低资源等工作模式，降低扫描对终端性能的影响。 支持扫描多层压缩包病毒能力，可自定义配置压缩包的扫描层数。 支持终端扫描到感染型病毒、顽固木马时，自动进入深度查模式，可设置禁止终端用户管理路径或文件白名单、禁止终端用户管理扩展名白名单、扫描时不允许终端用户暂停或停止扫描任务。 为提升病毒识别率，系统内置包括但不限于人工智能检测、启发式检测引擎、云查杀引擎、云规则检测引擎等可以灵活配置混合使用。
18.		安全准入系统	1、基本要求：支持办公网、视频监控网、物联网等多种终端设备类型的混合网络场景，实现设备发现、网络边界管理、入网控制、合规评估等泛终端准入控制管理功能，≥1000M 网络流量处理能力。授权管理数≥180 个，≥6 个千兆电口，≥4TB 硬盘，服务期内质保和升级。 支持与防病毒系统对接，实现单一控制中心统一管理的能力。 2、准入控制：支持多种认证控制方式，支持 802.1x、portal、DHCP、MAB MAC、策略路由、旁路镜像、WebAuth 等方式，支持无线和有线环境下的接入控制，适应复杂网络环境下的接入控制。 针对未认证或不合规的设备，当终端访问 http、https 网站时，支持对其网站访问重定向至引导页面进行身份认证或修复。 支持 LDAP、Email、Http 认证源三种认证源配置，支持第三方认证源的高可用配置；支持在不修改第三方认证源中用户信息的前提下，临时限制特定账号的入网认证请求。 支持员工扫描访客二维码和短信方式快速审批访客入网的访客认证方式；支持管理员修改资产清单中设备登记的资产信息字段。 通过小路由、VPN 等场景接入的经过 NAT 转换后的终端必须安装客户端并经过身份认证后方可接入网络。 支持手动或自动学习 IP/MAC 绑定关系，通过配置策略可对网络内设备随意变更 IP 地址的行为或随意使用其他设备 IP 地址的行为进行快速发现和有效阻断。 3、访问授权：可基于用户、角色、设备类型、设备分组、设备标签、终端安检结果等动态下发 VLAN、acl 或厂家属性。 支持基于不同设备类型定义访问控制规则，特定类型的设备仅允许访问指定的关键服务器，并只允许合法的协议通过。 支持基于终端使用用户的用户组、用户角色定义访问控制策略，无论用户使用什么设备还是 IP，均可执行对应的访问控制策略。

			4、合规检查：能检查终端外在静态指纹特征，支持多种特征维度，支持 DHCP 动态 IP 下的设备仿冒检查，无论非法设备修改 IP 还是修改 MAC 进行仿冒替换，系统均能快速发现并及时阻断。 支持全静默的终端身份认证，无需人工参与，终端即可自动完成准入认证，整个过程无弹窗，不影响全屏进程。 支持进程检查、共享文件检查、补丁检查、U 盘运行检查、软件检查、非法外联检查、操作系统检查、远程桌面检查、开放端口检查，并可对检查不合规的终端进行禁入网和不合规情况提示。 5、安全逃生：系统需具备多种逃生机制，一键认证放行、阈值检测逃生、第三方服务器异常自动放行，确保非正常情况下不影响用户网络的稳定运行。

7）销售网点综合安全接入服务

序号	名称		技术要求
1.	销售网点综合安全接入服务	主要服务内容	1、服务期内，利用销售网点综合安全接入平台提供全省销售网点的安全接入服务，所需的平台、工具和服务队伍由供应商提供，并满足最新的等级保护制度建设要求和行业安全建设要求。 2、销售网点综合安全接入平台包括但不局限于以下业务模块： （一）服务期内现有“综合业务安全接入系统”的运营维护； 包括如下工具： ①综合业务安全接入系统运行平台（2 套）； ②安全管理中心/安全注册认证中心（2 套）； ③业务均衡网关（2 套）； ④安全接入中心（2 套）； ⑤安全接入终端（4300 台）； ⑥防火墙（终端专用）（2 台）； 以上运营维护包括但不限于设备的质保、软件升级、定期巡检和应急响应（安全接入终端分布于全省各地市销售网点）。 （二）新增“综合业务安全接入系统”的工具部署，服务期内提供销售网点综合安全接入服务； 包括如下工具： ①综合业务安全接入系统运行平台（1 套）； ②安全管理中心/安全注册认证中心（1 套）； ③业务均衡网关（1 套）； ④安全接入中心（4 套）； ⑤安全接入认证软件（支持不超过 2000 套）； ⑥防火墙（终端专用）（1 台）； 以上工具部署和运营维护包括但不限于工具的现场实施、系统联调、定期巡检和应急响应（安全接入终端分布于全省各地市销售网点）。

			★为保证业务系统的稳定性与连续性，供应商需要承诺保证与现行“综合业务安全接入系统”无缝兼容（提供承诺函）；供应商需要承诺兼容市场现有安全接入终端设备，并满足新旧安全接入终端设备或安全接入认证软件的同时接入使用（提供承诺函）；供应商需要承诺满足全国性新游戏的安全接入，包括：通讯、认证和支付系统，可与中福彩行业安全通讯系统、安全认证系统、安全支付系统等进行无缝兼容和对接，符合《彩票管理条例》和彩票行业技术要求（提供承诺函）。 ★3、随着安全建设要求的不断提高，以及销售网点规模的不断扩大，在服务期内，供应商除提供上述“综合业务安全接入系统”以外，还需要根据业务实际情况不断新增和补充新的设备，以满足等级保护制度及行业的安全建设要求。**本项目不仅包括以上服务内容，而且还包括采购人由于信息系统变更、升级等衍生的新增服务内容（增量不超过以上服务内容的 10%），供应商需要提供相关承诺函。**
2.	销售网点综合安全接入服务技术指标要求	综合业务安全接入系统运行平台	1、组成：综合业务安全接入系统由安全管理中心、安全注册认证中心、业务均衡网关、安全接入中心组成。 ★2、硬件平台：不低于 6U 机框式万兆硬件平台，采用符合 PICMG3.0 标准的 ATCA 架构，该平台可通过热插拔物理板卡方式集成实现各种业务板卡协同工作，支持可插拔物理板卡数量不少于 5 个，设备标配双电源模块、双风扇模块，支持热插拔更换； 6U 6 槽双星 10G 背板 ATCA 架构； 标配 2 块 3000W 220V 交流电源模块； 智能风扇，每槽位散热 350W； 单槽 12 路 10GbE 业务面、12 路 GbE BASE 面交换板，背板带 6 个 GbE 电口 6 个 GbE 光接口。
3.		安全管理中心	1、组成 ：安全管理中心由安全管理软件和专用硬件平台组成。 2、软件要求 ：负责整个网络环境中安全接入设备的证书发放、身份认证和管理。 3、远程管理 ：支持安全管理中心管理端和安全管理中心服务端分别安装于不同的主机。 4、加密通信：支持对称 / 非对称相结合的数据加密方式，证书管理采用遵循 X.509 格式的数字证书作为认证载体；支持将安全管理中心服务端作为证书签发机构（CA）来使用。 5、设备管理：支持对用户接入服务管理器设备的增、删、改及分域管理；支持用户接入服务管理器设备在线状态监控，支持用户接入服务管理器设备的启用、禁用。 6、隧道管理：具备创建、修改、删除、启用和禁用隧道功能；具有容错功能，具有明确的错误提示功能，对于重要的参数被错误地更改时系统会自动恢复到原来正确的设置，防止因升级失败或其他异常操作造成系统无法正常工作。 7、通信策略管理：对用户接入服务管理器设备进行身份认证、统一管理。可以对整个业务网络中的隧道策略进行集中定义和下发，能够详细定义每条隧道的协商参数、认证方式、加密算法等。 8、在线监控：能够对用户接入服务管理器设备在线状态信息进行实时监控、当前网络地址信息监控、并对设备的隧道信息状态进行监控。 9、容错功能：具有明确的错误提示功能；对于重要的参数被错误地更改时系统会自动恢复到原来正确的设置；防止因升级失败或其他异常操作造成系统无法正常工作。 10、管理员管理 ：支持对管理员的管理和授权，支持管理员分级。

			11、分组管理 ：支持对用户接入服务管理器设备按照一定的规则分组进行管理。 12、审计功能：记录、统计整个系统的运作信息记录，统计管理员的历史操作进行审计，保障网络运行的安全提供有利的分析数据。 ★13、运行平台：基于 ATCA 架构的物理板卡方式，并根据实际应用物理板卡数量可叠加扩展，性能线性增加，支持热插拔；ATCA 架构；内部 2 路 10GbE 网口、2 路 GbE 网口；2 个外置 GbE 电口。 14、提供上述系统的《计算机软件著作权登记证书》。
4.		安全注册认证中心	1、组成 ：安全注册认证中心由安全注册认证软件和专用硬件运行平台组成。 2、软件要求：通过验证用户接入服务管理器设备的序列号、绑定的彩票机特征码、获取的证书号，对用户接入服务管理器设备进行初始化注册管理，保证每台用户接入服务管理器设备是有效的。 3、设备注册认证 ：具备对用户接入服务管理器设备的身份认证功能。 4、配置信息下载：具备对用户接入服务管理器设备自动下载所需信息进行配置功能，支持远程配置用户接入服务管理器设备功能。 5、设备证书下载 ：具有对用户接入服务管理器设备进行身份认证，分发临时证书功能。 6、信息自动修改 ：具备对用户接入服务管理器设备配置信息修改后自动下载功能。 7、设备信息绑定 ：具备对用户接入服务管理器设备上所需接入的彩票机特征信息绑定功能。 8、设备统一管理 ：具备对用户接入服务管理器设备统一管理功能。 9、软件统一自动升级 ：支持对用户接入服务管理器设备远程控制统一自动软件升级功能。 ★10、运行平台：基于 ATCA 架构的物理板卡方式，并根据实际应用物理板卡数量可叠加扩展，性能线性增加，支持热插拔（与安全管理中心运行在同一业务板上）ATCA 架构；内部 2 路 10GbE 网口、2 路 GbE 网口；2 个外置 GbE 电口。 11、提供上述系统的《计算机软件著作权登记证书》。
5.		业务均衡网关	1、组成 ：业务均衡系统由业务均衡软件和专用硬件运行平台组成。 2、软件要求：支持不同 ISP 链路接入，实现多链路均衡，确保用户 inbound 和 outbound 双向动态选路与均衡，为用户选择最优链路，提高链路品质。 3、部署方式：支持路由模式、透明模式和旁路模式部署，适用于各种复杂的网络环境；支持策略路由，能满足复杂环境下的部署。 4、多链路支持：支持多链路接入，能根据 ISP 智能选路；支持链路保持，使访问服务入站和出战链路保持一致。 5、链路均衡：支持动态链路均衡和热备，提高多运营商网络接入时网络可靠性支持入站/出站流量均衡，能根据链路健康度动态选路；内置 ISP 地址库和国内省份 IP 地址库，可依据 ISP、省份进行链路选择和均衡。 6、智能 DNS ：支持智能 DNS,无需第三方工具/服务即可实现智能 DNS 解析功能。 7、服务均衡 Layer4 均衡：支持应用负载均衡功能，支持平均分发，压力分发，请求分发等算法；支持全透明 L4 均衡，能保留原始客户端的地址支持三角传输模式均衡，服务响应不经过交付网关，避免应用交付设备成为瓶颈。 8、Layer7 均衡：支持 HTTP/HTTPS/RDP/常规 TCP 应用均衡发布，支持平均分发，压力分发，请求分发等算法；支持基于 HTTP 请求页面、请求参数和请求头对 WEB 服务器进行均衡；支

			持基于 Cookie 或 Session 对 WEB 均衡进行会话保持。 9、ESP 协议均衡 ：能够支持单独的 ESP 协议与 IPSEC 加密调度到相同的目的地址。 10、内容交换：支持基于规则的内容交换，可依据条件的逻辑判断结果或组合选择提供服务的服务器；条件支持请求头、请求页面、请求方法、客户端源地址、 COOKIE、服务端证书颁发者与 DN、客户端证书颁发者与 DN 等；逻辑判断支持等于、开始、结尾、包含、正则等方式可为应用服务器提供工作与备用机等多种服务模式。 11、应用加速与控制：支持 SSL 卸载，可以分担应用服务器 SSL 运算压力，有效提升服务器处理能；支持 SNI，允许多域名虚拟主机同时进行 SSL/TLS 认证支持与后台服务器基于 SSL 连接通信；应用加速：支持连接保持功能，实现多连接复用，减小服务器压力能对 Web 应用数据进行实时智能压缩，改善终端用户性能，提高带宽利用率；可灵活依据域名和 URI 对应用内容高速缓存，降低服务器 I/O 压力，提升页面响应速。应用控制：可定义每个服务器的最大并发连接和每秒连接能力，防护服务浪涌，避免过量请求造成服务器缓慢；可设置 TCP 保活、 TCP MSS、 TCP 连接回收、 TCP 内容缓冲的细粒度参数，适应不同形态的 WEB 应用。 12、健康检查：支持多种 ICMP、 TCP 和 HTTP 等健康检查方；支持自定义健康检查；支持对链路进行健康检查,能根据健康度动态均衡策略调整；支持对服务器进行健康检查，能根据健康度进行动态均衡策略调整。 ★13、运行平台 ：基于 ATCA 架构的物理板卡方式，并根据实际应用物理板卡数量可叠加扩展，性能线性增加，支持热插拔；ATCA 架构；内部 2 路 10GbE 网口、2 路 GbE 网口；4 个外置 GbE 电口。 14、提供上述系统的《计算机软件著作权登记证书》。
6.		安全接入中心	1、组成 ：中心用户接入服务管理器（安全接入中心）由安全接入软件和专用硬件运行平台组成。 2、软件要求：是面向福彩省级中心的万兆级安全接入系统，负责各销售终端安全接入服务器的安全接入和统一管理。 3、网络模式 ：支持多种网络接入，小区宽带、 ADSL、 DHCP 等。 4、安全传输功能：支持安全加密传输，支持 NAT 穿越；支持 3DES、 DES、AES 等多种加密算法；支持高速加密卡加速引擎；可根据用户需求定制加密算法； 5、加密隧道管理：支持与安全管理中心通信，实时自动下载加密隧道信息，实时查看隧道运行情况；加密隧道信息和非加密隧道信息的带宽管理；加密隧道密钥采用动态密钥协商技术，能够定期协商新的加密密钥。 6、访问控制 ：采用双重访问控制技术，具备阻断来自网络内部用户的攻击功能。 7、证书认证 ：支持数字证书。 8、防火墙功能：支持 DNS、 DDNS；支持双向 NAT；支持深层次状态检测，阻止来自应用层的攻击；支持 IP 与 MAC 地址绑定功能；支持时间、用户、协议、安全域、内容访问控制，防止常见的 DoS/DDoS 攻击。 9、设备管理功能：具备 WEB 方式的配置与管理功能；具备基于角色的分级管理功能；支持配置导入导出；具备分组日志审计功能。 10、配置管理 ：自动从安全注册认证中心下载配置信息。 ★11、运行平台：基于 ATCA 架构的物理板卡方式，并根据实际应用物理板卡数量可叠加扩

			展，性能线性增加，支持热插拔；ATCA 架构；内部 2 路 10GbE 网口、2 路 GbE 网口；2 个外置 GbE 电口。每秒最大并发隧道数>=2000 条。 12、提供上述系统的《计算机软件著作权登记证书》。
7.		安全接入认证软件	1、软件要求：支持安卓系统，是面向销售终端的专用安全接入软件，负责与现有综合业务安全接入系统建立加密隧道并进行安全通信和管理。 2、外联网络接入：支持 ADSL、专线、宽带、3G/4G 等多种静态/动态接入方式。 3、业务系统认证接入：支持彩票机接入身份认证以及特征码绑定，实现彩票机通过加密隧道接入业务系统。 4、远程认证管理：支持与安全注册认证系统通信，能够自动下载配置信息，能够通过系统进行软件的统一管理配置。 5、加密传输：支持与安全管理系统通信，能够自动下载设备的隧道信息，自动与安全接入系统建立安全加密传输隧道。 6、安全传输功能：支持 3DES、DES、AES 等多种加密算法；支持 SSL 链路自动检测；支持 SSL 加密 WiFi。 7、认证方式：支持数字证书认证方式。 8、自动更新：支持与注册认证系统通信以及安全管理系统通信，实现配置自动下载更新、策略自动分发；支持本地/远程升级。 9、扩展功能：需要与行业安全认证系统进行无缝兼容和对接，符合《彩票管理条例》和彩票行业技术要求，支持国密算法 SM1，SM2，SM3，SM4。提供厂商兼容福彩行业安全认证系统和二次开发承诺函原件。 10、提供上述系统的《计算机软件著作权登记证书》。
8.		防火墙（终端专用）	1、组成：防火墙软件及专用硬件运行平台组成 2、软件要求：负责综合业务安全接入系统的安全防护和控制 3、网络接入：支持 ADSL、专线、宽带、3G/4G 等多种静态/动态接入方式。 4、访问控制：可针对 IP、MAC、端口、时间对象设定基于应用、网络服务（非网络端口）的安全过滤 5、入侵防御：包括蠕虫/木马/后门/DoS/DDoS 攻击探测/扫描/间谍软件/利用漏洞的攻击/缓冲区溢出攻击/协议异常/IPS 逃逸攻击等。 6、DOS 防护：支持防御 SYNFlood、ICMPFlood、UDPFlood、TCP 报文标志位不合法攻击防范 7、应用识别：支持 1000 种应用，可以识别 P2P,OA，操作系统、网络协议、通讯工具、媒体软件、视频工具、游戏、下载工具等协议 8、流量管理：支持上下行带宽通道独享，支持 IP 带宽的平均分配、自由抢占，支持基于访问行为的目标 IP 的分配与管理 9、流量分析：能够识别统计不少于 200 种的应用流量，形成 TOP5 的统计 10、日志管理：支持访问控制、DOS 攻击、入侵检测、MAC 绑定、ARP 攻击、网络外连等多种安全日志查询，能够记录 IP 来源，目的 IP，源端口，目的端口协议 11、设备管理功能：具备 B/S 架构的配置界；支持统一集中管理；支持统一集中配置。 ★12、运行平台：≥2U 专用机架式硬件设备，冗余电源；不少于 1000BASE-T*6,SFP*2,RS232*1，可扩至 24 光或电接口，支持万兆；吞吐量：不小于 4Gbps；并发连接：不小于 5,000,000 新

			建连接：不小于 250,000。

8）等级保护测评服务

序号	名称		技术要求
1	等级保护测评服务	主要服务内容	1、服务期内，针对河南省福利彩票发行中心(河南省养老事业发展中心)销售网络及业务系统进行等级保护测评服务等专项安全服务，服务期间所需的相关设备、人员、服务和第三方费用（包括但不限于聘请具有等保测评资质的机构协助等）均由供应商负责，采购人不再承担与等级保护测评工作相关的任何费用。 2、服务期内，等级保护测评服务包括但不局限于以下服务内容： ①完成年度等级保护的定级、测评服务； ②完成在公安部门的等级保护备案工作； ③提供年度等级保护的定期自查服务等。 ★3、随着行业应用系统不断地增加，网络安全建设日益重要，在服务期内，需要根据用户的实际情况不断完善和补充，以满足等级保护及行业的安全建设要求。
2		主要服务措施	1、服务期内，按照等级保护政策文件的相关技术要求，进行等级保护的测评、整改、备案、自查等工作，包括但不局限于以下服务要求： ①进行等级保护的测评工作时，供应商需要完成生产系统（含电脑票热线销售系统和即开票销售系统）、计算机辅助管理系统（CAM）（含运营管理信息系统（OMIS）、办公自动化（OA）和渠道营销管理平台）、门户网站系统（河南福彩网）三个系统的定级、测评、备案工作； ②进行等级保护的整改工作时，供应商需要按照等级保护测评的结果进行整改和完善，并满足等级保护相关的要求； ③进行等级保护的自查工作时，供应商需要按照等级保护测评的标准和要求进行自查工作，并满足等级保护相关的要求。 ★2、以上具体服务内容依据等级保护最新要求、整改意见、行业应用要求和省中心实际情况提供整体服务内容，供应商需要提供服务期内确保我中心业务系统等保测评工作达标的承诺函。

9）年度专项攻防演练保障服务

序号	名称	技术要求

1	年度专项攻防演练保障服务	主要服务内容	1、服务期内，提供针对河南省福利彩票发行中心(河南省养老事业发展中心)销售网络及业务系统展开的专项攻防演练需要提供安全服务保障，服务期间所需的相关设备、人员和服务均由供应商负责。 2、服务期内，年度专项攻防演练保障服务包括但不局限于以下服务内容： ①在相关部门展开专项攻防演练时提供驻场服务； ②资产梳理与风险发现； ③安全监测与应急响应； ★3、随着行业应用系统不断地增加，网络安全建设日益重要，在服务期内，需要根据用户的实际业务要求不断完善和改进，以满足等级保护及行业的安全建设要求。
2		主要服务措施	1、服务期内，在相关部门展开专项攻防演练时提供安全服务，包括但不局限于以下设备、人员和服务： ①设备包括但不局限于网络资产测绘分析系统（公安部一所网探 D01 或同类设备）、网络攻击阻断系统（公安部一所网盾 K01 或同类设备）、网络违规外联稽查系统（公安部一所网联 E01 或同类设备）； ②人员包括但不局限于以下要求：提供一线驻场服务人员 3 人,二线非驻场服务人员不少于 5 人的技术服务人员，服务人员应为业务骨干，具有计算机相关证书或专业技术资格条件，熟悉河南福彩业务及相关政策的专业团队，服务期间，负责网络安全、安全审计、网点安全设备维护等方面的工作，其中驻场人员与客户共同建立攻防演练行动安全保障小组，明确组内成员职责，建立畅通沟通机制。 ③服务内容包括但不局限于以下要求： 1） 行动开展前：a.协助制定《攻防演练工作部署方案》以及《应急处置方案》。b.资产梳理与风险发现，全面了解和掌握系统面临的信息安全威胁和风险。c.加强防护能力。d.加强监测与应急处置能力。 2） 行动开展中：a.落实值班制度，安排专人负责安全巡检。b.预警监测与关联分析研判，发现安全事件立即启动应急响应流程，对异常 IP 进行溯源并封禁，同时对风险点进行加固。 3） 行动结束后：a.协助客户对工作中发现的问题成果进行梳理，对攻击途径、攻击方式、防守成果进行总结。b.下一步工作计划制定，对发现的信息系统安全隐患制定《信息安全加固方案与计划》在下一阶段安全工作中进行不断完善。 ★2、以上具体服务内容、时间、次数依据攻防演练发起单位要求、行业应用安全要求和省中心实际情况提供专项的攻防演练安全服务，供应商需要按照用户要求保质保量的完成。**供应商需要提供承诺函**。

10）安全运维驻场服务

序号	名称	技术要求

1	安全运维驻场服务	主要服务内容	1、服务期内，提供针对本项目涉及的各业务系统和各项工作提供安全运维和驻场服务，服务期间所涉及的相关设备、人员和服务由供应商提供。 2、服务期内，安全运维驻场服务包括但不局限于以下服务内容： ①定期巡检安全检查服务； ②紧急事件安全应急服务； ③重大事件安全值守服务； ④安全评估渗透测试服务； ⑤安全漏洞通报服务； ⑥安全策略优化服务； ⑦新业务上线前安全检测； ⑧本地化运维支撑服务； ★3、随着行业应用系统不断地增加，网络安全建设日益重要，在服务期内，需要根据用户的实际情况不断完善和补充服务内容，以满足等级保护及行业的安全建设要求。
2		主要服务措施	1、服务期内，提供安全巡检，应急响应和驻场服务，包括但不局限于以下服务内容： ①定期巡检安全检查服务：针对销售网络安全服务平台的月度安全巡检、季度安全巡检等，并提供巡检报告。 ②紧急事件安全应急服务：针对紧急发生的安全事件、黑客攻击做应急等，并提供应急报告。 ③重大时间安全值守服务：重要节假日安全值守，主管部门安全检查、攻防演练等，提供安全值守服务。 ④安全评估渗透测试服务：定期针对生产系统（含电脑票热线销售系统和即开票销售系统）、计算机辅助管理系统（CAM）（含运营管理信息系统（OMIS）、办公自动化（OA）和渠道营销管理平台）、门户网站系统（河南福彩网）三个系统开展安全漏洞扫描和渗透测试服务。 ⑤安全漏洞通报服务：提供安全通告，掌控最新的安全漏洞和安全态势，同步排查清除相应的安全隐患，做到防患于未然。 ⑥安全策略优化服务：定期进行综合分析研判，并针对性优化安全策略，保障各业务区域安全防护策略的合理性和有效性。通过定期升级及策略优化，以达到最佳的安全防护效果。 ⑦新业务上线前安全检测：新业务上线前进行安全检测，包括主机与应用的漏洞检测、渗透测试等,并协助相关应用厂商进行整改加固。 ⑧本地化运维支撑服务：集中服务期，提供一线驻场服务人员 3 人,二线非驻场服务人员不少于 5 人的安全服务专业团队。提供完善的客户培训计划。提供完善的安全服务文档和安全服务记录，建立安全服务档案。 ★2、以上具体服务内容依据等级保护最新要求、行业应用安全要求和省中心实际情况提供安全运维驻场服务，在业务需求增加时根据实际情况及时补充服务人员，本项目不仅包括以上服务内容，而且还包括采购人由于信息系统变更、升级等衍生的新增服务内容（增量不超过以上服务内容的 10%），**供应商需要提供相关承诺函**。

（5）运营维护服务

1）运营维护服务范围

序号	类别	名称	规格型号	生产厂商	数量
1	中心设备	TSAS 硬件平台	TSAS-1000	西安天泰创新科技有限公司	2 台
2		安全管理中心和安全注册认证中心	TRM-1000HN	西安天泰创新科技有限公司	2 块
			天泰 TSM 安全管理软件[简称：TSM]V1.0)	西安天泰创新科技有限公司	2 套
			天泰 TRM 安全注册认证软件[简称：TRM]V1.0	西安天泰创新科技有限公司	2 套
3		业务均衡网关	TBG-1000HN	西安天泰创新科技有限公司	2 块
			天泰业务均衡软件[简称：TBG]V1.0)	西安天泰创新科技有限公司	2 套
4		安全接入中心	TSG-1000HN	西安天泰创新科技有限公司	2 块
			天泰安全接入软件[简称：TSG/C]V2.0	西安天泰创新科技有限公司	2 套
5		防火墙	SGFW-T1-2000P	上海天泰网络技术有限公司	1 台
		防火墙	TNFW-2000P	西安天泰创新科技有限公司	1 台
6	终端设备	终端用户接入服务管理器	TSG-100HN	西安天泰创新科技有限公司	4300 台
			天泰安全接入软件[简称：TSG/C]V1.0	西安天泰创新科技有限公司	4300 套

2）运营维护服务要求

通过定期对“综合业务安全接入系统”中心及终端设备进行检查、检修和维护，确保系统安全运行。

在服务期内，供应商应提供 7*24 小时的维护维保服务，在接到采购人报修通知后，服务人员持续跟进直到故障排除后设备完全恢复正常使用为止。特殊情况下供应商应提供备用设备，确保服务范围内所约定的软硬件系统正常运转。遇到重大技术问题，及时组织有关技术专家进行会诊，并采取相应措施以确保正常运行。

在服务期内，供应商应严格要求服务人员不得使用不符合技术要求和质量要求的零配件，同时认真做好服务记录，记录维修前故障和修理后的设备质量状况；维修完毕，请采购人检验修理后的设备和服务

记录。

供应商应保证常用维修配件的合理储备，确保维护维保工作的正常进行，避免因缺少零配件而延误维修时间。

当服务范围内所约定的软硬件系统发生故障时，供应商应及时进行设备维修与更换。供应商应设立备件库进行备件支持，对故障件维修并及时更换不能现场修复的设备。

供应商应根据维护维保服务记录，定期提交服务报告，归类总结服务期内的故障和采购人提出的问题，对于带有普遍性的问题及时予以重点解决，同时供应商应定期进行维护巡检，以及时发现并处置故障。

供应商应根据采购人需求定期提供健康检查、系统巡检、专项维护等服务，并通过监测和分析，及时发现设备中存在的问题和隐患。针对隐患，供应商采取防范措施加以预防；针对发现的问题，应果断采取处置措施；最后提交相应的服务报告。

供应商应根据采购人需求进行软件升级和健壮性配置优化；所有软件优化升级必须按照采购人要求先进行部分销售网点测试，测试成功后再进行全省销售网点的优化升级。

供应商应根据采购人要求进行相关技术培训。

供应商所有技术操作应获得采购人授权后执行。

供应商提供日常维护及应急响应服务。

（6）安全保密要求

1）★信息保密、网络安全要求。中标供应商及服务人员要履行国家法律法规规定的相关保密义务，遵守采购人保密规定和网络安全规定。服务人员在未经过采购人相关人员认可的情况下，不得将任何采购人认为涉及数据安全的观点、数据、系统结构信息、测试结论以及测试记录传播、披露和使用。未经采购人同意，中标供应商不得擅自修改任何程序和数据。中标供应商及其服务人员须与采购人分别签订保密协议。

2）服务人员应熟悉所系统及系统运行环境，详细了解系统软件、组件、操作系统等品牌、型号和版本信息。服务人员应了解上述软件、组件的安全状态，及时从对应官方网站获知相关漏洞和补丁信息，并第一时间告知采购人相关人员。服务人员应按照采购人要求及时升级补丁，修复漏洞。

1.4 项目验收方案要求

项目验收工作由采购人按照验收的有关制度和流程组织开展。中标供应商在合同约定的时间向采购人提出验收申请，采购人负责审核是否满足项目验收准入条件。满足验收准入条件后，予以启动项目验收程序。

（1）项目验收准入条件

1）合同约定的时间段内，本项目采购需求中提出的服务内容全部完成。

2）服务方式、服务质量、服务成果以及组织管理和项目文档满足本项目投标文件的规定。

（2）项目验收标准

采购人以本项目采购需求中相关内容为依据，作为项目验收标准。中标供应商是否按照本项目投标文件中定义的各项服务内容、服务要求开展各项工作，工作流程和结果是否符合采购人质量管理要求，是否在规定时间内提交相关工作文档。

（3）项目验收流程

符合项目验收准入条件后，供应商可提出项目验收申请。验收流程如下：

1）供应商提出项目验收申请，并按要求提交运维相关文档资料。

2）采购人组织进行项目验收评审，对项目工作内容及文档进行验收评审。

3）项目验收评审通过后，采购人出具项目验收报告。

（4）验收交付物

中标供应商需要按照采购人要求，提交相关符合质量要求的工具、软件、组件、文档。

2.商务要求

2.1 报价要求

本次报价须为人民币报价，包含：本项目实施完成价（包括：维护和维保服务所需的设备、材料、人员、相关服务费、税费和相关费用等完成此项目的所有费用）。对在合同实施过程中可能发生的其它费用（如：增加耗材、材料涨价、人工、运输成本增加等因素），采购人概不负责。对于本文件未列明，而供应商认为必需的费用也需列入总报价。在合同实施时，采购人将不予支付供应商没有列入的项目费用，并认为此项目的费用已包括在总报价中。

2.2 服务时间

不少于 365 天，具体服务周期以总预算除以单日服务费报价后取整位数确定。

2.3 服务地点

河南省福利彩票发行中心(河南省养老事业发展中心)指定地点（包括但不限于省中心机房及全省各地市销售网点）

2.4 付款条件

本合同签订后，于服务起始日前二十个工作日内,乙方向甲方支付合同价款 3%的履约保证金（履约保证金户名：河南省福利彩票发行中心(河南省养老事业发展中心)，账号：246801819248，开户行：中行金水支行）。甲方在收到履约保证金且乙方出具合法发票后十五个工作日内，甲方向乙方支付合同总价款的 100%。待维护期满（按日历计算）后三十个工作日内，甲方向乙方一次性无息返还 3%的履约保证金。发票是付款的先决条件，如乙方无提供发票，甲方有权拒绝支付合同款。

2.5 质量要求

达到国家及行业合格标准和采购人要求。

2.6 其它要求

提供至少应包含销售网络基础安全防控服务、销售网络安全加固服务、销售网点综合安全接入服务、年度等级保护测评服务、年度驻场运营维护服务的技术服务方案。

2.7 知识产权

供应商须保证采购人在中华人民共和国境内使用其提供的服务或其任何一部分时，享有不受限制的无偿使用权，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律或经济纠纷。如供应商不拥有相应的知识产权，则在投标总价中必须包括合法获取该知识产权的一切相关费用，如因此导致采购人损失的，供应商须承担全部赔偿责任。供应商如欲在项目实施过程中采用自有知识成果，须在响应文件中声明，并提供相关知识产权证明文件。

第六章 竞争性磋商响应文件格式

封面格式

竞争性磋商响应文件

项目名称：
项目编号：
供 应 商：_____（企业电子公章）
法定代表人或被授权代理人：_____（个人电子签章或签字）

目录

供应商自行编制目录包括标题、页码

一、商务部分

1、资格证明文件

1-1、具备独立承担民事责任的能力法人资格

提供（第二章 供应商须知 附件一、初步评审内容）本项的相关证明的截图或复印件或扫描件（企业电子公章）

1-2、具有良好的商业信誉和健全的财务会计制度

提供（第二章 供应商须知 附件一、初步评审内容）本项的相关证明的截图或复印件或扫描件（企业电子公章）

1-3、有依法缴纳税收和社会保障资金的良好记录

提供（第二章 供应商须知 附件一、初步评审内容）本项的相关证明的截图或复印件或扫描件（企业电子公章）

1-4、履行合同所必需的货物和专业技术能力的书面声明

本单位郑重声明：

我单位在参加（项目名称）采购活动中，有履行本项目的人员、设备、资金、信用等能力。

供应商（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

1-5、在经营活动中没有重大违法违规记录的书面声明

本单位郑重声明：

我单位在参加采购活动前三年内在经营活动中没有《政府采购法》第二十二条第一款第(五)项所称重大违法记录，包括：

我单位或者其法定代表人、董事、监事、高级管理人员未因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚，或者存在财政部门认定的其他重大违法记录，以及在财政部门禁止参加采购活动期限以内的情况。

特此声明！

供应商（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

1-6、无不良信用记录承诺

本单位郑重承诺，我单位无以下不良信用记录情形：

1.被人民法院列入失信被执行人；

2.被税务部门列入重大税收违法失信主体名单；

3.被政府采购监管部门列入政府采购严重违法失信行为记录名单。

我单位已就上述不良信用行为按照磋商文件中磋商须知前附表规定进行了查询。我单位承诺：合同签订前，若我单位具有不良信用记录情形，贵方可取消我单位成交资格或者不授予合同，所有责任由我单位自行承担。同时，我单位愿意无条件接受监管部门的调查处理。

供应商（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

附：信用查询记录

说明：由于电子交易平台的特殊性，投标截止之间之前无法获得供应商名单，供应商应于投标截止时间前通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）等渠道查询信用记录，可自愿将查询的信用结果网站截图附在响应文件内。投标截止开启后当日，由采购人或代理机构进行供应商信用查询，并将查询结果网站截图上传交易平台。查询的信用结果以采购人或代理机构查询的为准。

1-7、无行政及经济关联或利害关系的承诺

本单位郑重承诺：

我单位在参加政府采购活动，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，未参加同一合同项下的政府采购活动。与采购人及相关代理机构没有行政及经济关联或利害关系。没有为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务，未参加该采购项目的其他政府采购活动。未联合体参加本次项目。

供应商（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

1-8、政府采购政策落实

1-8-1、中小微企业声明函

（服务）

（提供或填写；盖公章）

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。企业的具体情况如下：

1、信息安全服务，属于 软件和信息技术服务业 ；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[1]，属于（选择：□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。

供应商（盖公章）：_____

日期：_____年____月____日

说明：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.填写前请认真阅读“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）”文件、“财政部 工业和信息化部关于印发《政府采购促进中小企业发展管理办法》的通知（财库[2020]46 号）”文件的规定。

1-8-2、监狱企业证明材料

（若是，提供或填写；不是，保留格式，可不填写，不盖章）

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

供应商（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

1-8-3、残疾人福利性单位声明函

（若是，提供或填写；不是，保留格式，可不填写，不盖章）

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（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

2、法定代表人身份证明或授权委托书

2-1、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。

附：法定代表人身份证原件截图或影印件或复印件

供应商（企业电子公章）：
法定代表人（个人电子签章或签字）：

2-2、授权委托书

（法定代表人参加本次项目活动，可不出具次委托书）

声明：（供应商全名）的（法定代表人姓名、职务）代表本公司授权（被授权人的姓名、职务）为本公司的合法代理人，就（项目名称），（项目编号：）的竞争性磋商事宜。

特此声明。

附：法定代表人身份证复印件及被授权代理人身份证原件截图或影印件或复印件

供应商（企业电子公章）：

法定代表人（个人电子签章或签字）：

被授权代理人（个人电子签章或签字）：

3、报价函

致：（采购人名称）

根据贵方（项目名称）竞争性磋商公告，供应商（供应商名称、地址）提交按采购文件供应商须知部分要求提供的加密电子响应文件 1 份。

据此函，宣布同意如下：

1.若我方通过评审并最后报价承诺，此报价为所提供本项目采购及服务所需的全部费用。

2.供应商将按采购文件的规定履行合同责任和义务。

3.供应商已详细审查全部采购文件，包括修改文件（如有的话）以及全部参考资料和有关附件。我们完全理解并同意放弃对这方面有不明及误解的权利。

4.供应商同意按照贵方的要求提供与本报价有关的一切数据或资料，完全理解贵方并无义务必须接受最低报价的报价或收到的任何报价。

5.与本报价有关的一切正式往来通讯请发往：

地址：

电话：　　传真：

供应商（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

3-1、磋商首次报价

3-1-1、首次报价一览表

供应商名称	
单日报价 （元）	大写：
	小写：￥
服务期限 （服务期）	
响应有效期 （有效期）	
保证金	0
质量要求	
备注	交易平台的首次报价和最后报价，均应填写单日报价。 单日报价和总价的所报价格计算保留小数点后两位，四舍五入。

供应商（企业电子公章）：
法定代表人或被授权代理人（个人电子签章或签字）：

3-1-2、分项价格表

序号	项目名称	项目内容	单日金额（元）	单日金额乘以服务期得出总价（元）
1	销售网络基础安全防控服务	建立覆盖全省的销售网络基础安全防控服务平台，通过平台为各业务区提供综合防控服务，符合行业安全建设的要求。包括但不限于建设态势感知平台、威胁情报联防平台、销售网点运维管理平台等专用平台及配套的服务，满足等级保护的要求。		
2		核心业务区安全防控服务：通过基础安全防控服务平台，为核心业务区提供相关工具和防控服务，符合行业安全建设的要求。包括但不限于电脑票、即开票等销售系统的综合防控，满足等级保护的要求。		
3		辅助业务区安全防控服务：通过基础安全防控服务平台，为辅助业务区提供相关工具和防控服务，符合行业安全建设的要求。包括但不限于中福彩中心、各级福彩机构、销售网点等业务接入管理，满足等级保护的要求。		
4		外联业务区安全防控服务：通过基础安全防控服务平台，为外联业务区提供相关工具和防控服务，符合行业安全建设的要求。包括但不限于银行、运营商、新渠道等外联单位的业务接入管理，满足等级保护的要求。		
5		外部办公区安全防控服务：通过基础安全防控服务平台，为外部办公区提供相关工具和防控服务，符合行业安全建设需要。包括但不限于外部办公业务、互联网业务等安全接入管理，满足等级保护的要求。		
6	销售网络安全加固服务	提供覆盖全省的销售网络安全加固服务，通过提供相关工具和防控服务，建设符合行业安全的要求。包括但不限于防火墙、入侵防御、漏洞扫描、网络审计、数据库审计、日志审计、WEB 应用防火墙、高级持续性威胁检测与管理系统、防病毒、准入系统、堡垒机等通用安全设备及配套的服务，满足等级保护的要求。		
7	销售网点综合安全接入服务	提供覆盖全省的销售网点综合安全接入服务，通过提供相关工具和防控服务，建设符合行业安全的要求，包括但不限于对现有“综合业务安全接入系统”中心设备及全省传统销售网点已部署终端设备的运营维护，以及涵盖全省渠道销售网点的安全接入，满足等级保护的要求。		
8	年度等级保护测评服务	完成生产系统（含电脑票热线销售系统和即开票销售系统）、计算机辅助管理系统（CAM）（含运营管理信息系统（OMIS）、办公自动化（OA）和渠道营销管理平台）、门户网站系统（河南福彩网）三个系统的年度等保定级、测评，以及在公安部门的备案等相关工作，满足等级保护的要求及行业安全建设的要求。		

9	年度驻场运营维护服务	专项攻防演练保障服务：在服务期内，根据公安部门、民政部门及中福彩中心等行业主管部门的要求，提供配合开展专项安全检查进行的攻防演练等配套服务工作，提供现场服务保障，具体保障时间与行业主管部门的要求一致。		
10		系统安全运维驻场服务：针对本项目涉及的系统提供人员驻场服务，包括但不限于对中心机房和销售网点提供定期巡检、安全检查、应急响应等运维服务，以及对软件工具、病毒库、漏洞库和特征库等进行升级迭代跟踪及更新服务。		

说明：（1）供应商详细项目类别报价或费用的可单独列明，未单独列明分项报价或费用的将视为包含在总报价中，合同执行中不另行支付。本表根据内容可续页。

（2）最后报价后，分项价格的价格按（首次报价－最后报价)除以首次报价后得出的优惠率视同分项价格的优惠浮动值(特定分项价格除外)。此优惠率调整原则适用于合同内价格的计算及项目增减、变更时价格的计算。由于电子交易平台的特殊性，供应商也可在平台系统提交最后报价时，在附件总上传最后分项价格表。

供应商（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

4、商务条款响应偏离表

序号	商务条款要求	是否响应	偏离说明
1	完全理解并接受对供应商完成项目服务范围、服务要求、服务期限、服务地点、质量要求、其它要求、知识产权等商务内容的服务要求。		
2	完全理解并接受对供应商的各项须知要求和责任义务。		
3	报价内容均涵盖报价要求之一切费用和伴随服务；所提供的报价为总报价，即完成整个合同项目有关的所有费用。		
4	所提供的报价不高于采购预算金额。		
5	完全理解并接受合同条款及格式所列述的各项条款。		
6	同意按本项目要求缴付相关款项或付款条件。		

注：1.根据“第五章采购需求和服务要求 一商务要求”和采购文件中汇总的上述主要商务要求，如供应商完全响应的，在“是否响应”栏内填写“完全响应”，并在“偏离说明”栏中填写“无偏离”；如供应商有未响应或部分未响应的，在“是否响应”栏内填写“未响应或部分未响应”，并在“偏离说明”栏中填写“正偏离或负偏离，同时描述其偏离情况的内容”。

2.本表根据内容可续页。

供应商（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

5、其他

5-1、反商业贿赂承诺书

我公司承诺：

在（项目名称）采购活动中，我公司保证做到：

一、公平竞争参加本次采购活动。

二、杜绝任何形式的商业贿赂行为。不向国家工作人员、政府采购代理机构工作人员、评审专家及其亲属提供礼品礼金、有价证券、购物券、回扣、佣金、咨询费、劳务费、赞助费、宣传费、宴请；不为其报销各种消费凭证，不支付其旅游、娱乐等费用。

三、若出现上述行为，我公司及参与采购的工作人员愿意接受按照国家法律法规等有关规定给予的处罚。

供应商（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

5-2、承诺函

我公司承诺：

在____（项目名称）_____项目（项目编号：_____）采购活动中，我公司保证做到：

1、我方提交的响应文件内容均真实、合法有效，不提供虚假材料。

2、在响应文件递交截止时间后，投标有效期内不撤销或修改响应文件。

3、如若我方成交，在收到成交通知书后，如无正当理由将在规定的时间内与采购人签订合同。

4、如若我方成交，我方将按采购文件中规定的提供履约保证金或履约担保（如有）。

5、如若我方成交，我方在签订合同时不向采购人提出附加条件。

6、如若我方成交，我方将按照采购文件规定向采购代理机构一次性缴纳招标代理服务费。

7、我方完全按照采购文件要求，所发布的内容符合国家行业最新规范标准要求。

8、在报价及实施中涉及的文字、图片、音像内容为原创或有相关授权，并承诺保证采购人在使用我方成果时不承担涉及任何专利权、商标权、著作权或其他知识产权的法律责任，否则，由此引起的全部法律责任由我公司承担。

我单位若有违反上述承诺内容，愿承担相应责任，愿意接受采购人、相关监督部门作出的包括但不限于取消投标/成交资格、实施不良行为记录、限制投标、公开曝光及相关的行政处理、处罚。

供应商（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

5-3、成交服务费承诺

致：（采购代理机构 ）

本单位郑重承诺：

在参加____（项目名称）_____项目（项目编号_____）中若获成交供应商，我们保证在领取《成交通知书》6 个工作日内，按文件的规定，以电汇、转账、现金方式按规定向贵公司一次性支付应该交纳的成交服务费用。

供应商（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

二、技术部分

2-1、技术响应与偏离表

采购文件条目号		内容要求	响应文件应答	偏离说明
1.1 项目概况	（1）项目背景	……见采购需求和服务要求 一技术要求		
	（2）项目目标	……见采购需求和服务要求 一技术要求		
	（3）项目内容	……见采购需求和服务要求 一技术要求		
	（4)安全服务内容一览表	……见采购需求和服务要求 一技术要求		
1.2 对投标（响应）文件的基本要求		……见采购需求和服务要求 一技术要求		
1.3 项目实施	（1）项目建设要求	1）需要满足信息中心建设发展 ……见采购需求和服务要求 一技术要求		
		2）需要按照新的等级保护制度要求建设 ……见采购需求和服务要求 一技术要求		
		3）需要制定适合福彩行业的安全建设方案 ……见采购需求和服务要求 一技术要求		
		4）需要实施不同区域的安全策略 ……见采购需求和服务要求 一技术要求		
		5）需要建立河南福彩行业整体防护体系 ……见采购需求和服务要求 一技术要求		
		6）需要建立覆盖全省的运维管理平台 ……见采购需求和服务要求 一技术要求		
		7）需要建立专业团队进行网络及安全运维 ……见采购需求和服务要求 一技术要求		
	（2）时间要求	……见采购需求和服务要求 一技术要求		
	（3）服务团队要求	……见采购需求和服务要求 一技术要求		
	（4）技术指标要求	1）销售网络基础安全防控服务 ……见采购需求和服务要求 一技术要求		
		2）核心业务区安全防控服务 ……见采购需求和服务要求 一技术要求		
		3）辅助业务区安全防控服务 ……见采购需求和服务要求 一技术要求		
		4）外联业务区安全防控服务 ……见采购需求和服务要求 一技术要求		

		5）外部办公区安全防控服务 ……见采购需求和服务要求 一技术要求		
		6）销售网络安全加固服务 ……见采购需求和服务要求 一技术要求		
		7）销售网点综合安全接入服务 ……见采购需求和服务要求 一技术要求		
		8）等级保护测评服务 ……见采购需求和服务要求 一技术要求		
		9）年度专项攻防演练保障服务 ……见采购需求和服务要求 一技术要求		
		10）安全运维驻场服务 ……见采购需求和服务要求 一技术要求		
	（5）运营维护服务	1）运营维护服范围 ……见采购需求和服务要求 一技术要求		
		2）运营维护服务要求 ……见采购需求和服务要求 一技术要求		
	（6）安全保密要求	……见采购需求和服务要求 一技术要求		
4	1.4 项目验收要求	（1）项目验收准入条件 ……见采购需求和服务要求 一技术要求		
		（2）项目验收要求 ……见采购需求和服务要求 一技术要求		
		（3）项目验收流程 ……见采购需求和服务要求 一技术要求		
		（4）验收交付物 ……见采购需求和服务要求 一技术要求		

注：1、对照“第五章采购需求和服务要求 一技术要求”进行响应。全部响应的在“响应文件应答”栏注明“完全响应”，同时，在“偏离说明”栏中注明“无偏离”；如有偏离的请对应 “技术参数要求”栏中内容在“响应文件应答”栏中对应逐条应答明，同时，在“偏离说明”栏中注明“正偏离”或“负偏离”情况。偏离情况按评分办法标准要求进行对应分值扣除。

2.本表根据内容可续页。

供应商（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

2-2、实施方案

根据第五章 采购需求和服务要求和评审要求可进行相应的响应。
内容不限，自拟响应格式。

2-3、相关服务承诺

根据第五章 采购需求和服务要求和评审要求可进行相应的响应。
内容不限，自拟响应格式。

三、供应商认为需要提供的其它内容

说明：可附供应商认为评审所需或必要的补充资料证明的复印件或扫描件，并加盖单位公章。等等

3-1、业绩

（若有，请填写和提供；否则，保留格式，可不填写和提供）

序号	签约时间	项目名称和内容	合同金额	用户联系电话	备注
1					
2					
3					
	……				

注：按照顺序提供合同及发票并加盖供应商公章相关证明资料的原件截图或扫描件或复印件。本表根据内容可续页。

供应商（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

3-2、拟派服务人员

序号		姓名	职务	年龄	学历	工作经验年限	职称或相关资格能力水平证书（如有）			备注
							证书名称	证号/级别	专业/类别	
一线驻场人员	1									
	2									
	3									
	……									
二线非驻场人员	1									
	2									
	3									
	4									
	5									
	……									

附：需提供以上有效的人员工作简历（包括工作时间、承担工作内容、证明人联系方式等内容）的证明材料和相关证书扫描件并加盖供应商公章，本表根据内容可续页。

供应商（企业电子公章）：

法定代表人或被授权代理人（个人电子签章或签字）：

3-3、其他

……

交易中心平台信息库相关表格

投标人基本情况表

附：

序号	证书名称

企业资质信息

企业资质信息	
序号	资质等级名称

附：

序号	证书名称

企业业绩信息

企业业绩信息				
序号	工程名称	建设单位	合同签订时间	合同金额

附：

项目扫描件：

序号	证书名称	查看

企业各类证书信息

企业各类证书信息	
序号	证书名称

序号	证书名称	查看

企业财务情况

企业财务情况	
序号	年度

序号	证书名称	查看

企业社保及纳税情况

附：

序号	材料名称	查看

其他投标材料

其他投标材料	
序号	材料名称

序号	证书名称	查看