甘肃省政府集中采购

单一来源采购文件

采购文件编号：GJDY202022

项目名称：甘肃省福利彩票发行管理中心福利彩票网络安全综合防控服务政府采购项目

采 购 人：甘肃省福利彩票发行管理中心

集采机构：甘肃省公共资源交易局

2021 年 1 月.兰州

目　录

第一章 协商通知

甘肃省公共资源交易局对甘肃省福利彩票发行管理中心福利彩票网络安全综合防控服务政府采购项目以单一来源方式进行采购。本项目经专家论证并已在甘肃省政府采购网进行单一来源公示，经财政部门审批为单一来源采购。

1.项目编号：GJDY202022

2.采购内容：

包号	采购内容
1	福利彩票网络安全综合防控服务

3.采购总预算：580 万元

4.实施单一来源采购的简要理由：

根据甘肃省人民政府办公厅甘政办发〔2019〕96 号文规定，故采用单一来源采购方式。故本项目拟定的唯一的供应商为：丝绸之路信息港股份有限公司。

5.供应商未被列入“信用中国”网站(www.creditchina.gov.cn)记录失信被执行人或重大税收违法案件当事人名单或政府采购严重违法失信行为记录名单；不处于中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为信息记录中的禁止参加政府采购活动期间的方可参加本项目的投标。

6.获取单一来源采购文件的时间、地点、方式：

2021 年 1 月 7 日至 2021 年 1 月 11 日,每日 00:00-23:59，社会公众可通过甘肃省公共资源交易网免费下载或查阅采购文件。拟参与甘肃省公共资源交易活动的供应商需先在甘肃省公共资源交易网上注册，获取“用户名+密码+验证码”，以软认证方式登录；也可以用数字证书（CA）方式登录。这两种方式均可进行“我要投标”等后续工作。详见《甘肃省公共资源交易网》首页“下载中心”中“电子服务系统 v2.0 电子版操作说明”，下载标书的网站：甘肃省公共资源交易网（http://ggzyjy.gansu.gov.cn/）。

7.信息注册、投标须知

为了规范交易平台的业务流程以及给用户提供方便快捷的服务，凡是拟参与甘肃省公共资源交易活动的招标人、招标代理机构、投标人需先在甘肃省公共资源交易网上注册，使用“用户名+密码+验证码”或 CA 数字认证方式登录办理业务。

社会公众可通过甘肃省公共资源交易网浏览公告，并点击“免费下载招标文件”，

根据系统提示，保存电子标书文件至本地电脑；投标人浏览电子标书后，确定投标的需登录甘肃省公共资源交易电子服务系统 2.0，在系统首页最新招标项目中查询需要投标的项目或在“招标方案”-“标段（包）”中查询需要投标的标段，选中后点击“我要投标”，根据要求填写信息。并依据系统生成的投标“保证金打款账号”交纳投标保证金；投标人可登陆甘肃省公共资源交易电子服务系统 2.0，在首页点击“保证金查询”按钮查询保证金信息或在甘肃省公共资源交易局网站“保证金查询”栏目查询。

8.递交响应文件截止时间、采购时间、地点及方式：

提交响应文件哈希值截止时间：2021 年 1 月 12 日 9 时 00 分前成功上传提交到”甘肃省公共资源交易局网上开标系统”（网址：http://121.41.35.55:3010/OpenTender/），对迟于投标截止时间提交的电子报价文件哈希值将不予接受。

采购时间： 2021 年 1 月 12 日 9 时 00 分

采购地点：甘肃省公共资源交易局第一电子谈判室

9.投标方式：本项目通过”甘肃省公共资源交易局网上开标系统”进行采购。投标供应商采用网上电子投标方式，集采机构不接受投标供应商递交的纸质报价文件，投标供应商将固化的电子报价文件（含其对应的哈希值）按采购文件要求成功上传提交到”甘肃省公共资源交易局网上开标系统”。

10. 投标保证金账户内容及递交须知：

投标保证金账户内容：

户　名：甘肃省公共资源交易局

账　号：以报名时收到的短信内容为准

开户银行：甘肃银行兰州市高新支行

行　号：3138 2105 4001

甘肃银行查询电话：0931-8276931

投标保证金到账截止时间：以采购文件要求的递交响应文件截止时间为准。

为保证开标现场对投标保证金到账情况进行核对，提醒投标人要充分考虑汇款及到账所需时间以及发现问题后采取补救措施所需时间，以确保投标保证金在规定时间前到账。因不能在投标截止时间前到达指定账户的，导致投标无效的后果由投标人自行承担。

投标保证金递交须知：

（1）投标人登记拟参加的项目成功后，系统会将投标保证金收款信息发送至投标

人报名时预留的手机；投标人也可登录甘肃省公共资源交易网自行查询。

（2）投标人必须从基本账户以电汇方式提交保证金，且投标保证金单位名称必须与投标人登记的单位名称一致，不得以分公司、办事处或其他机构名义递交。

（3）投标人在办理投标保证金电汇手续时，应按标段（包）逐笔递交保证金，投标保证金其他问题，可查看甘肃省公共资源交易网“投标保证金办理指南”。

（4）如有保证金办理相关问题，投标供应商请及时致电：0931-2909190,0931-2909303 咨询办理。

11.公告期限

采购公告的期限为 3 个工作日。即自 2021 年 1 月 7 日至 2021 年 1 月 11 日。

12.项目联系人姓名及电话：

采 购 人：甘肃省福利彩票发行管理中心

地　　址：安宁区万新南路 1 号

联 系 人：王彦军

联系电话：15693313555

集采机构：甘肃省公共资源交易局

地址：甘肃省兰州市城关区雁兴路 68 号

联 系 人：刘沛　　胡望定

联系电话：0931-2909252　　2909250

第二章 协商须知

协商须知前附表

条款号	条款名称	编列内容规定
一、说明		
1.1	采购项目	甘肃省福利彩票发行管理中心福利彩票网络安全综合防控服务政府采购项目
2.1	采购人	采 购 人：甘肃省福利彩票发行管理中心 地　　址：安宁区万新南路1号 联 系 人：王彦军 联系电话：15693313555
2.2	集采机构	集采机构：甘肃省公共资源交易局 地址：甘肃省兰州市城关区雁兴路 68 号 联 系 人：刘沛　　胡望定 联系电话：0931-2909252　　2909250
二、响应文件的编写		
13.1	响应文件有效期	60 天
14.1	响应文件数量	**固化的电子报价文件1份（含其对应的哈希值）。**
三、电子响应文件的递交		
16.1	递交响应文件方式、截止时间	本项目采用网上电子投标方式，不接受投标供应商递交的纸质投标响应文件，投标供应商将固化的电子投标响应文件（含其对应的哈希值）按采购文件要求，于 2021 年 1 月 12 日 9:00 时（递交响应文件截止时间）前成功上传提交到”甘肃省公共资源交易局网上开标系统”（网址：http://121.41.35.55:3010/OpenTender/），对迟于递交响应文件截止时间提交的电子投标响应文件哈希值将不予接受。
16.1	响应时间和采购地点	响应时间：同递交电子响应文件哈希值的截止时间。 采购地点：甘肃省公共资源交易局第一电子谈判室

16.2	投标保证金	金　额：50000 元（伍万元整） **投标保证金账户内容：** 户　名：甘肃省公共资源交易局 账　号：以报名时收到的短信内容为准 开户银行：甘肃银行兰州市高新支行 行　号：3138 2105 4001 甘肃银行查询电话：0931-8276931 投标保证金到账截止时间：以采购文件要求的递交响应文件截止时间为准。 为保证协商现场对投标保证金到账情况进行核对，提醒供应商要充分考虑汇款及到账所需时间以及发现问题后采取补救措施所需时间，以确保投标保证金在规定时间前到账。因不能在投标截止时间前到达指定账户的，导致投标无效的后果由投标人自行承担。 **投标保证金递交须知：** （1）供应商登记拟参加的项目成功后，系统会将投标保证金收款信息发送至投标人报名时预留的手机；供应商也可登录甘肃省公共资源交易网自行查询。 （2)供应商必须从基本账户以电汇方式提交保证金，且投标保证金单位名称必须与投标人登记的单位名称一致，不得以分公司、办事处或其他机构名义递交。 （3）供应商在办理投标保证金电汇手续时，应按标段（包）逐笔递交保证金，投标保证金其他问题，可查看甘肃省公共资源交易网“投标保证金办理指南”。 （4）如有保证金办理相关问题，投标供应商请及时致电：0931-2909190,0931-2909303咨询办理。

四、成交结果信息公布与供应商质疑		
23.1	财政部门指定的媒体	甘肃政府采购网、甘肃省公共资源交易网
26.1	履约保证金	无
五、其他相关要求		
无		

协商须知

一、说明

1.适用范围

1.1 本单一来源采购文件仅适用于单一来源采购文件第二章“协商须知前附表”中所叙述的采购项目。

2.定义

2.1 “采购人”是指依法进行政府采购的国家机关、事业单位、团体组织。本次政府采购的采购人名称、地址、电话、联系人见协商须知前附表。

2.2 “集中采购代理机构”（以下简称集采机构）是指甘肃省公共资源交易局。集采机构地址、电话、联系人见协商须知前附表。

2.3 “供应商”是指响应单一来源采购文件要求、参加单一来源协商采购的法人、其他组织或者自然人。

2.4 “采购小组”是指依据《中华人民共和国政府采购法》和财政部《政府采购非招标采购方式管理办法》有关规定组建，依法依规履行其职责和义务的机构。

2.5“单一来源采购文件”是指由集采机构发出的文本、文件，包括全部章节和附件及答疑会议纪要。

2.6 “响应文件”是指供应商根据单一来源采购文件向集采机构提交的全部文件。

2.7 “采购文件”是指包括采购活动记录、采购预算、协商文件、响应文件、评审报告、成交供应商确定文件、合同文本、验收证明、质疑答复、投诉处理决定及其他有关文件、资料。

2.8 “货物”是指各种形态和种类的物品，包括原材料、燃料、设备、产品等，详见《政府采购品目分类目录》(财库[2013]189 号)。

2.9 “工程”是指建设工程，包括建筑物和构筑物的新建、改建、扩建、装修、拆除、修缮等，详见《政府采购品目分类目录》(财库[2013]189 号)。

2.10 “服务”是指除货物和工程以外的其他政府采购对象，详见《政府采购品目分类目录》(财库[2013]189 号)。

2.11“节能产品”是指财政部和国家发展改革委员会公布现行的《节能产品政府采购品目清单》（财库[2019]19 号）中“★”标注的品目产品。“环境标志产品”是指财政部、环境保护部发布现行的《环境标志产品政府采购清单》（财库[2019]18 号）中的品目产品。

2.12 “进口产品”是指通过中国海关报关验放进入中国境内且产自关境外的产品，详见《关于政府采购进口产品管理有关问题的通知》(财库[2007]119 号)。

2. 13. 知识产权

2.13. 1 供应商应保证在本项目使用的任何产品和服务（包括部分使用）时，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由供应商承担所有相关责任。

2.13.2 采购人享有本项目实施过程中产生的知识成果及知识产权。

2.13.3 供应商如欲在项目实施过程中采用自有知识成果，需在响应性文件中声明，并提供相关知识产权证明文件。使用该知识成果后，供应商需提供开发接口和开发手册等技术文档，并承诺提供无限期技术支持，采购人享有永久使用权。

2.13.4 如采用供应商所不拥有的知识产权，则在报价中必须包括合法获取该知识产权的相关费用。

2.13.5 采购人、集采机构和竞争性谈判小组对供应商提交的响应性文件及其内容负有保密义务，未经对方书面同意，不得泄露或提供给第三人。

2.14 “书面形式”是指任何手写、打印、印刷的各种函件或具有法律效力的数据电文形式。

3.供应商的资格要求

3.1 供应商应当符合协商须知前附表中规定的下列资格条件要求；

（1）《政府采购法》第二十二条第一款规定的供应商基本资格条件及符合《单一来源采购公告》中关于供应商资格要求的规定。（本项目已在《甘肃政府采购网》进行了单一来源论证公示，且已经政府采购行政主管部门审批为单一来源采购，评审时无须进行资格审查。）

3.2 供应商不得存在下列情形之一：

（1）与采购人、集采机构存在隶属关系或者其他利害关系。

（2）除联合体外，法定代表人或单位负责人为同一个人或者存在直接控股、管理关系的不同供应商，不得同时参加同一项目或同一子项目的采购。如同时参加，则评审时将同时被拒绝。

（3）《中华人民共和国政府采购法实施条例》第十九条规定的内容。

3.3 关于中小微企业

中小微企业是指符合《中小企业划型标准规定》的供应商，通过协商提供本企业的

服务，或者提供其他中小微企业制造的服务。中小微企业应提供《中小微企业声明函》；提供其他中小微企业服务的，应同时提供其他中小微企业的《中小微企业声明函》。

根据财库〔2014〕68号《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》，监狱企业视同小微企业。监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地(设区的市)监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业投标时，提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件，不再提供《中小微企业声明函》。

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，残疾人福利性单位视同为小型、微型企业。

4.参与协商的费用

4.1 无论协商的结果如何，供应商应自行承担所有与采购活动有关的全部费用。

5．授权委托

5.1 供应商代表为供应商法定代表人的，应提供法定代表人身份证明。供应商代表不是供应商法定代表人的，应提供法定代表人授权书，并附法定代表人身份证明及委托代理人身份证明。

6.采购进口产品

6.1 经财政监管部门审核管理，并经进口论证后方可采购进口产品。

7.联合体形式

7.1 本次单一来源采购不接受为联合体形式的供应商。

7.2 供应商为联合体形式的，除应符合本章第 3 条规定外，还应遵守以下规定：

（1）联合体各方必须签订联合体协议书，明确联合体牵头人和各方的义务、工作、合同工作量比例；

（2）联合体各方均应当符合本章第 3.1 款规定的供应商基本资格条件；

（3）除**协商须知前附表**中另有规定，联合体各方中至少有一方应当符合本章第 3.1 款规定的供应商特定资格条件；

（4）联合体各方不得再单独或与其他供应商组成新的联合体参加同一项目的采购活动。

二、单一来源采购文件

8．单一来源采购文件的组成

8.1 单一来源采购文件由下列文件及在采购过程中发出的澄清或者修改文件组成：

第一章协商通知

第二章协商须知

第三章政府采购合同

第四章采购需求

第五章响应文件组成

第六章政府采购项目供应商满意度问卷

9. 单一来源采购文件的澄清或者修改

9.1 集采机构对已发出的单一来源采购文件进行必要澄清或者修改的，将以书面形式通知供应商。澄清或者修改文件作为单一来源采购文件的组成部分。

三、响应文件的编写

10.一般要求

10.1 供应商应仔细阅读单一来源采购文件的所有内容，按单一来源采购文件的要求编制响应文件，并保证所提供的全部资料的真实性，以使其响应文件对单一来源采购文件做出实质性的响应。

10.2 供应商提交的响应文件及供应商与集采机构、采购小组就有关协商的所有来往函电均使用中文。供应商可以提交其它语言的资料，但有关响应内容附中文注释，在有差异时以中文为准。

10.3 计量单位应使用我国法定计量单位。

10.4 响应文件应采用书面形式，电报、传真、电子邮件形式的响应文件概不接受。

10.5 供应商应按单一来源采购文件中提供的响应文件格式填写。

11.响应文件的组成

11.1 响应文件包括下列内容：

（1）协商响应声明

（2）供应商的资格证明文件

（3）商务/技术响应与偏离表

（4）售后服务承诺书

（5）报价明细表

（6）供应商认为需提供的其他资料

11.2 根据《中华人民共和国政府采购法》第四十二条的规定，供应商无论成交与否，其响应文件不予退还。

12.报价

12.1 供应商应当根据单一来源采购文件要求和范围报价。报价货币为人民币，以元为单位，保留小数点后两位。

12.2 供应商应按第四章“采购需求”要求及第五章“响应文件组成”格式填写。

12.3 供应商的最后报价不得超过采购项目预算，采购项目预算或其计算方法见协商须知前附表。

13.响应文件有效期

13.1 响应文件有效期见**协商须知前附表**，从本章第 17.1 项规定的递交响应文件截止之日起算。

13.2 特殊情况下，集采机构可于响应文件有效期满之前要求供应商同意延长有效期，要求与答复均应为书面形式。供应商可以拒绝上述要求而其保证金不被没收。供应商同意该要求，将要求其相应延长保证金的有效期。有关退还和没收保证金的规定在响应文件有效期的延长期内继续有效。

14.响应文件的签署及规定

14.1 供应商应按“协商须知前附表”要求提供固化的电子响应文件 1 份（含其对应的哈希值）。

14.2 电子响应文件为加盖电子公章或加盖鲜章后扫描后，使用投标文件固化工具固化后的格式，固化的电子响应文件应保证能正常读取，否则造成的一切后果由供应商自行承担。

14.3 响应文件的书写应清楚工整，任何行间插字、涂改或增删，必须由供应商的法定代表人或委托代理人签字或盖个人印鉴。字迹潦草、表达不清或可能导致非唯一理解的响应文件可能视为无效文件。

14.4 响应文件应根据采购文件的要求制作，签署、盖章和内容应完整，如有遗漏，将被视为无效报价。

14.5 响应文件统一用 A4 幅面编制。

14.6 供应商必须提供法定代表人和委托代理人的身份证复印件，委托代理人如在协

商现场进行必要的澄清或答疑时还必须出示身份证原件以确认其有效身份，否则将视为无效报价。

14.7 在协商过程中，供应商按采购文件规定和采购小组要求在规定的时间内提交的最后报价，可打印或用不褪色墨水书写，但需经法定代表人或其委托代理人签字，或者加盖供应商单位公章。否则，将导致响应文件无效。

四、响应文件的递交

15.响应文件的补充、修改或者撤回

15.1 供应商在协商须知前附表规定的递交响应文件截止时间之前，可以书面通知对其响应文件进行补充、修改或者撤回，该通知应由供应商法定代表人或其委托代理人签字。补充、修改的内容与响应文件不一致时，以补充、修改的内容为准。

15.2 在协商须知前附表规定的递交响应文件截止时间后，供应商不得对响应文件补充、修改或者撤回。

16.响应文件的递交与接收

16.1 供应商应在协商须知前附表规定的递交响应文件截止时间前，按照协商须知前附表 17.1 的要求递交响应文件，对迟于递交响应文件截止时间提交的电子投标响应文件哈希值将不予接受。

16.2 本次采购不接受邮寄的响应文件。

五、协商

17.协商程序

17.1 协商程序：对响应文件的资格性、符合性进行审查；响应文件的澄清；协商；推荐成交供应商。

18.响应文件的资格性、符合性审查

18.1 采购小组对响应文件进行资格性和符合性审查。响应文件有下列情况之一的将导致无效响应，供应商应进行补充或修改，使之符合单一来源采购文件要求：

（1）应交未交保证金或金额不足的；

（2）未按照单一来源采购文件规定要求签署、盖章的；

（3）响应文件有效期不足的；

（4）不符合法律、法规、规范性文件和单一来源采购文件规定的。

19.响应文件的澄清

19.1采购小组在对供应商提交的响应文件的有效性、完整性和对单一来源采购文件的响应程度进行审查时，可以以书面形式要求供应商对响应文件中含义不明、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、说明或者纠正。供应商的澄清、说明或者补正应当采用书面形式，由其法定代表人或其委托代理人签字。

19.2 错误修正的原则：报价大写金额和小写金额不一致的，以大写金额为准；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；单价金额小数点有明显错位的，应以总价为准，并修改单价。按上述原则修正的响应文件，对供应商起约束作用。

19.3 供应商应按采购小组通知的时间、方式，指派专人进行澄清、说明或者补正。

20.协商

20.1 采购小组与供应商进行价格协商，在保证采购项目质量的基础上，商定合理的成交价格。

20.2 商定价格，供应商可以进行多轮报价。对于能准确掌握同类项目同业同期平均价格（市场平均价）的，采购小组可要求供应商报出不超过市场平均价的合理价格；不能准确掌握市场价格的，双方可按供应商价格清单及说明协商价格，并以供应商近期其他中标或成交项目合同作为价格协商参考依据。

20.3 供应商的最终报价高于同业同期平均价格（市场平均价）的，采购小组可视情况接受或不接受。供应商响应文件实质性响应单一来源采购文件要求的，且未超过采购预算，则应确认成交，但采购小组应出具相关书面材料说明接受该报价的理由，并报财政部门备案；采购小组不接受的，采购小组应出具相关书面材料说明的理由，采购终止。

20.4 采购终止后，重新开展采购活动。

21.协商终止

21.1 协商时，出现下列情况之一，本次协商终止：

（1）因情况变化，不再符合规定的单一来源采购方式适用情形的；

（2）出现影响采购公正的违法、违规行为的；

（3）报价超过采购项目预算的。

21.2 采购小组应将协商终止理由通知供应商。

22.保密要求

22.1 采购小组成员以及与协商工作有关的人员对协商情况以及协商过程中获悉的国家秘密、商业秘密应当保密。

六、成交结果信息公布与授予合同

23.成交信息的公布

23.1 协商结束后，成交结果信息将在财政部门指定的媒体上公布。指定的媒体名称见**协商须知前附表**。

24.询问

24.1 供应商对政府采购活动事项有疑问的，可以向采购人或集采机构提出询问。采购人或集采机构将及时作出答复。

25.成交通知

25.1 成交供应商确定后，集采机构将以书面形式向成交供应商发出成交通知书。成交通知书对采购人和成交供应商具有同等法律效力。

25.2 成交通知书是合同文件的组成部分。

26.履约担保

26.1 成交供应商在收到集采机构的成交通知书后十日内，应按照**协商须知前附表**的规定，向采购人提交履约担保。联合体成交的，履约担保由联合体各方或联合体中牵头人的名义提交。（如有）

26.2 成交供应商没有按照本章第 27.1 项规定提交履约担保的，视为放弃成交，其保证金不予退还。

27.签订合同

27.1 单一来源采购文件、成交供应商的响应文件及其补充的响应文件等均为签订政府采购合同的依据。

27.2 成交供应商应当在成交通知书发出之日起三十日内与采购人签订政府采购合同。

27.3 成交供应商应当按照合同约定履行义务。成交供应商不得向他人分包成交项目。

七、其他规定

28.采购代理服务费

28.1 集采机构不收取采购代理服务费。

29.成交通知书的领取。

29.1 成交供应商在成交公告发布后 7 个工作日内在甘肃省公共资源交易局九楼政府采购处领取成交通知书，不另行通知。

30.其他规定

30.1 单一来源采购文件的其他规定见协商须知前附表。

第三章　政府采购合同格式条款

政府采购合同

合同编号：　HT-(采购文件编号)
项目名称：
采购文件编号：

甲方：
乙方：
集采机构：

年　　月

一、政府采购合同协议书

采购合同编号：HT-(招标文件编号)

采购人（全称）：_____（甲方）

供应商（全称）：_____（乙方）

为了保护甲、乙双方合法权益，根据《中华人民共和国合同法》、《中华人民共和国政府采购法》和《中华人民共和国政府采购法实施条例》及其他有关法律、法规、规章，双方签订本合同协议书。

1.项目信息

（1）项目名称：_____

（2）招标文件编号：_____

（3）项目内容：_____

2.合同金额

（1）合同金额小写：_____

大　　写：_____

（2）合同价格形式：固定总价合同　　。

3.履行合同的时间、地点及方式

4.付款：

5.解决合同纠纷方式

首先通过双方协商解决，协商解决不成，则通过以下途径之一解决纠纷：

□ 提请仲裁　　□ 向人民法院提起诉讼

6.组成合同的文件

本协议书与下列文件一起构成合同文件，如下述文件之间有任何抵触、矛盾或歧义，应按以下顺序解释：

（1）在采购或合同履行过程中乙方做出的承诺以及双方协商达成的变更或补充协议

（2）中标通知书

（3）投标文件

（4）政府采购合同格式条款及其附件

（5）专用合同条款

（6）通用合同条款

（7）标准、规范及有关技术文件

（8）其他合同文件。

7.合同生效

本合同自_____生效。

8.合同份数

本合同一式____份，采购人执___份，供应商执___份，均具有同等法律效力。

合同订立时间：_____年_____月_____日

合同订立地点：_____

甲方（公章）： 地址： 电话: 邮编: 法定代表人或委托代理人： 签字日期:　　年　　月　　日 经 办 人: 签字日期:　　年　　月　　日 开户行： 账号：	乙方（公章）： 地址： 电话: 邮编: 法定代表人或委托代理人： 签字日期:　　年　　月　　日 经 办 人: 签字日期:　　年　　月　　日 开户行： 账号：

二、合同通用条款

服务类政府采购合同格式文本省级以上政府部门或行业组织有标准或示范文本的，应按照其文本确定合同格式。没有文本的，按照《中华人民共和国合同法》及采购项目特点自行拟定特定文本确定合同格式。

第四章　采购需求

一、招标内容

1、项目招标内容一览表

序号	项目名称	项目内容	数量	时间	地点
1	网络安全基础安全防控服务	建立覆盖全网的网络安全基础安全防控平台，提供相关设备和防控服务，满足行业安全建设的要求，包括但不限于大数据安全分析平台、网络集中管理平台、数字证书认证平台等专用安全平台，以及下一代防火墙、入侵防御系统、WEB 应用防火墙、数据库审计系统、上网行为管理系统、漏洞扫描系统、堡垒机、网络准入控制系统、防病毒系统、综合日志审计系统等通用安全产品，满足等级保护要求。	1 套	合同签订生效之日起 50 日内	用户指定地点
2	核心业务区安全防控服务	在核心业务区提供相关设备和防控服务，满足行业安全建设的要求，包括电脑票、即开票销售系统、视频票销售系统、视频票监控等综合防控服务，满足等级保护的要求。	1 套		
3	支撑业务区安全防控服务	在支撑业务区提供相关设备和防控服务，满足行业安全建设的要求，包括中福彩中心、地市中心、投注站等业务接入管理，满足等级保护的要求。	1 套		
4	外联业务区安全防控服务	在外联业务区提供相关设备和防控服务，满足行业安全建设的要求，包括银行、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。	1 套		
5	外部办公区安全防控	在外部办公区提供相关设备和防控服务，并满足行业安全建设需要，包括外部办公业务、官网官微、运营管理、互联网业务等安全接入管理，满足等级保护的要求。	1 套		

	服务				
6	网络安全专项服务	提供针对网络安全展开的专项安全服务，包括安全设备升级维护服务，协助进行等级保护的测评、整改、自查工作，以及相关部门的专项攻防演练等综合安全服务。	3 年		

二、项目建设需求

2.1、项目建设背景

近几年，随着房租、人力成本的急剧增加，投注站的生存压力越来越大，站点开始尝试引进其他业务以增加销售收入；社会化渠道顺势也进入福彩行业，开始出现了彩票兼营或自助等新型网点。不但彩票销售网点变得复杂、多样，彩票销售系统也变得复杂、多样。但彩票销售网点的兼营化、彩票销售主体的社会化、彩票销售业务的信息化是未来发展趋势，我们必须面对。由于彩票销售网点变得复杂、多样，网络安全问题也日益突出。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，对我省福彩信息化管理又提出了更高的要求。等级保护 2.0 除了具体“技术要求”外，还有相对应的“管理要求”。这就要求我们在进行“技术要求”建设的同时，也要在“管理要求”上进行完善。安全建设需要大量的安全技术人员，包括安全评估、安全加固、应急响应等不同专业技能的人员。我省中心技术人员不仅在数量上严重不足，而且在安全技能上专业度也不够，而主系统供应商主要负责彩票销售系统和自有设备终端的维护，再加上庞大的彩票销售网点和复杂的社会化渠道供应商，网络及安全运维变得困难。

面对中心业务系统越来越多、越来越复杂，各种类型彩票销售网点数量越来越多、情况越来越复杂，而我们的管理体系和建设方式也需要进行大幅度的调整，仅仅依靠人工和传统的管理，已经很难维护起来这么复杂的业务系统，急需建立起覆盖我省的福彩销售系统综合防控服务平台，并形成以“产品+平台+服务”为主体的多层次、立体的动态防御体系。安全是相对的、动态的和需要持续建设的，不同时期有不同时期的安全要求，考虑到我省中心技术人员本来就严重不足，专业安全技术人员更是缺乏，一次性建设资金投入也较大。我省中心从实际情况出发，采用安全服务托管方式，建立起我省福彩销售系统综合防控服务体系，以满足国家相关法律法规和福彩行业的要求，同时又满足我省福彩实际业务的需求。

2.2、项目建设要求

2.2.1、业务需求

（一）需要按照新的等级保护制度要求建设

《网络安全法》明确规定信息系统运营、使用单位应当按照网络安全等级保护制度要求，履行安全保护义务。随着新的等级保护制度的施行，等级保护 2.0 在等级保护 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。福彩行业作为公众服务性行业，涉及亿万彩民和重要数据信息，一旦出现安全问题，将会造成恶劣影响和不可挽回的损失，需要在新的等级保护制度要求下进行建设和完善。

（二）需要制定适合福彩行业的安全建设方案

福彩业务作为“类金融”系统，数据流、资金流和彩民信息需要有严密的安全保障体系。网络安全建设过程中，一定要根据行业的特点制定适合福彩行业的安全建设方案。安全性和易用性有时候是一对矛盾，作为面向公众、服务大众的业务系统，涉及面广、关注度高，安全建设既要符合国家有关法律法规的要求，也要考虑业务系统的易用性。

（三）需要针对业务类型实施不同安全策略

根据等级保护制度的要求，首先对我省福彩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设备、安全措施和安全服务手段等。

（四）需要建立我省福彩行业整体防护体系

网络安全一定要强调整体性，否则一个环节出现漏洞，整体安全防护就会出现重大问题。对于福彩来说，虽然省中心机房及核心业务非常重要，也是防护重点，但上千个投注站却是薄弱环节，也最容易疏忽。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。

（五）需要建立覆盖全省的福彩运维管理平台

我省福彩网络结构复杂，既有电脑票、即开票等销售系统，也有运营管理系统、官网官微等服务系统，还有银行、电信运营商、新渠道商等外联单位，以及上千个各类投

注站。从销售系统、服务系统、外联单位以及投注站都可以到达省中心和中福彩中心，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，更需要建立起覆盖我省的运维管理服务平台和工具，形成以“产品+平台+服务”为主体的运维管理体系。

（六）需要建立专业团队进行网络及安全运维

等级保护 2.0 除了具体“技术要求”外，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。安全建设需要大量的安全技术人员，省中心技术人员不仅在数量上严重不足，而且在安全技能上专业度也不够。需要借助第三方建立一支既熟悉福彩行业又熟悉网络安全的专业团队驻地进行网络及安全运维服务。

2.2.2、项目实施建设要求

序号	实施内容	计划时间	成果及验收标准
1	需求分析	合同签订生效之日起 10 日内	根据等级保护要求、整改意见及需求，提出安全建设实施方案，并交付甲方确认。
2	项目建设	合同签订生效之日起 30 日内	按照甲方确认的安全建设实施方案，进行该项目的实施，并交付甲方进行试运行。
3	项目交付	合同签订生效之日起 50 日内	系统交付及相关文档的完善和递交。 甲方或指派第三方完成项目验收。
4	服务期限	合同签订生效之日起三年内	按照销售网络安全防控服务要求，提供 3 年期的综合安全防控服务。

三、技术指标要求

3.1、网络安全基础安全防控服务

3.1.1、网络安全基础安全防控服务总体要求

序号	名称	技术要求
1	网络安全基础安全防控服务总体要求	1、服务期内，所需的基础安全平台、安全产品和服务队伍由中标方提供，并满足等级保护 2.0 的建设要求、行业安全建设要求和定制开发要求。 2、网络安全基础安全防控服务包括但不局限于以下三部分：网络安全基础安全防控平台及定制开发、通用安全产品加固和网络安全专项安全服务。 ① 大数据安全分析平台（1 套，覆盖全网，含定制开发）； ② 网络集中管理平台（1 套，覆盖全网（含投注站），含定制开发）； ③ CA 数字证书认证平台（1 套，覆盖全网，含定制开发）； ④ 下一代防火墙（9 台）； ⑤ 入侵防御系统（4 台）； ⑥ WEB 应用防火墙（1 台）； ⑦ 数据库审计系统（1 台）； ⑧ 上网行为管理系统（1 台）； ⑨ 漏洞扫描系统（1 台）； ⑩ 堡垒机（1 台）； ⑪ 网络准入控制系统（1 台）； ⑫ 防病毒系统（1 套，120 个 PC 端，80 个服务器端）； ⑬ 综合日志审计系统（4 台）； ⑭ 网络安全专项安全服务（3 年期）。 ★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，网络安全基础安全防控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。**供应商需要提供承诺函。**

3.1.2、网络安全基础安全防控平台及定制开发要求

序号	名称	技术要求	
1	大数据安全分析平台	大数据安全分析系统	1、采用先进、成熟、适用并符合未来发展趋势的大数据技术，同时保障应用技术的稳定性、扩展性、安全性、开放性、灵活性、易用性和便捷性；支持基于 CDH 开源平台的部署，便于兼容 Hadoop 与其他开源项目的集成和执行端到端的大数据工作流程。 ★2、内置态势感知模块，能够满足基于行业应用的安全态势感知的要求，覆盖到全省 3000 多个投注站安全接入终端。**供应商需要提供承诺函。** ★3、内置日志审计模块，能够满足基于等级保护要求的日志审计的要求，覆盖到全省 3000 多个投注站安全接入终端。**供应商需要提供承诺函。** 4、支持分级部署、分级管理模式，以便适应用户的管理制度和组织架构；支持服务器集群技术，可实现在线动态扩充，以便于随着业务需求的增长系统性能能够随着系统服务器数目的增加从而实现平滑线性增长。 5、支持主流安全设备、网络设备、主机设备、中间件、数据库、应用系统等日志采集，包括但不限于：WINDOWS、LINUX、防火墙、IPS/IDS、WAF、漏洞扫描、nginx、apache、DNS 设备等，支持多种采集协议，包括 Syslog、JDBC/ODBC、NETCAT、FTP/SFTP、TCP/UDP 等；支持对接 KAFKA 方式采集数据。 6、范式化解析规则覆盖范围涵盖常见设备和应用类型，包含但不限于主机、防火墙、IPS/IDS、WAF、网络设备、安全设备、数据库、应用系统、中间件等多种设备和系统的日志范式化解析能力。 7、范式化数据解析支持正则、分隔符、JSON 格式 key=value 键值、JSON+正则组合等解析方式支持数据清洗、过滤，支持字段的静态替换和补全；支持对异构原始数据进行统一格式化处理，对于被标准化后的数据保存原始日志。

			8、支持数据存储至 ElasticSearch、Hbase、HDFS；支持数据存储至 Kafka，便于第三方系统对接。 9、支持允许用户自定义增加、删减图表仪表盘，以及每个仪表盘的位置和大小、背景色、刷新频率等内容；支持增加多个展示标签页，每个标签页可任意引用多个已定义好的仪表盘组件；通过直观且可交互查询的图表，帮助安全分析人员简便快捷发现难于发现的威胁和风险。 10、支持数字、环比、仪表板、表格、环图、雷达图、柱状图、折线图、趋势图、象限图、迁徙图、省份分布、世界分布、图片、URL 嵌入、sparkline、趋势分析、桑基图、树形图等方式满足用户对所选数据进行展示的要求。支持根据灵活的配置展示组件内的数据计算逻辑，并能够确保数据源选择、过滤条件设定、时间控件设定的逻辑与其他功能模块一致。 11、支持自定义规则策略配置，支持五种以上的策略计算框架（包括但不限于：having count distinct、having sum、having avg、follow by、next 等）支持对事件、依赖事件的区分。 ★12、大数据防控分析平台行业对接：根据行业不同业务类型定制建立不同的大数据防控分析业务，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。**供应商需要提供承诺函。** ★13、需提供原厂商的产品技术规格表和产品图片。
2		运行平台	★①主运行平台采用基于 ATCA 架构 7U 万兆电信级设备，本设备符合 PICMG3.0 标准，6 槽双星架构，10G 背板，可通过热插拔物理模块方式集成实现各种业务板卡协同工作。标配 2 块 3000W 220V 交流电源模块。标配 1 块基于 ATCA 架构的万兆交换板，12 路 10GbE 业务面、12 路 GbE BASE 面交换模块，背板带 6 个 GbE 电口、6 个 GbE 光接口。标配 1 块基于 ATCA 架构的业务板，支持热插拔，不低于 E5 系列六核双路 CPU，不小于 64G 内存，内置 64GSSD，至少 2 路 10GbE 网口、2 路 GbE 网口、2 个外置 GbE 电口。②存储服务器：三台机架式服务器，不低于 2U 高度，配置不低于：英特尔至强 E5-2620V4，内存≥32G，硬

			盘≥2T，硬盘类型：SAS，磁盘陈列卡：H730-1G 缓存，光驱：DVDRW*1，750W 双电源，导轨*1。
3		定制开发	①态势分析模块投注站安全运营页：需要建立实时监测投注站与省中心、中福彩中心的安全态势感知平台，通过内置的安全态势模块与站点综合安全接入系统进行无缝对接和联动，将站点安全接入终端、各类销售终端的日志进行收集和导入，建立起覆盖站点的安全态势感知系统。 ②态势分析模块安全态势运营页：提供平台新增事件，事件处置维度、资产管控维度、考核指标等模块看版，支持基于地理位置、事件级别、事件类型、处置时间进行筛选查询，支持以日／周／月／年为查询周期。 ③态势大屏-综合态势模块：提供整体安全态势展示，含攻击态势地图，事件总量与已确认的事件量、资产管控量、日志接入量、内网安全、威胁源 IPTOP10、外部威胁（按攻击类型）、被攻击目标 IPTOP5、内外网攻击趋势、事件威胁级别占比，时间周期支持日／周／月数据切换。 ④态势大屏-内网安全模块：提供内网安全态势展示，含内部受攻击主机排名、内部恶意攻击源、攻击事件所处杀伤链统计、系统受威胁情况、内网攻击趋势、内网攻击实时滚动事件、内网事件威胁级别占比、内部资产评分、漏洞数量、事件量统计，时间周期支持日／周／月数据切换； ⑤态势大屏-互联网安全模块：提供互联网态势展示，含全球攻击 IPTOP5、被攻击域名 TOP5、攻击类型展示、域名攻击源区域 TOP10、被攻击最多的 URLTOP5、互联网攻击趋势、互联网攻击实时滚动事件、互联网事件威胁级别占比，时间周期支持日／周／月数据切换展示。 ★以上①②③④⑤项供应商需要提供定制开发承诺函，并承诺在合同签订后 30 日内完成，符合甲方或指派第三方项目验收条件。
4	网络	运维	1、产品能够部署在 Windows 和 Linux 操作系统上，具备自主知识产权

	集中管理平台	区网络集中管理平台	的通用软件平台，具备高可靠高扩展性等特点。 2、内置数据库，包即包含系统平台框架、资产管理、安全事件管理、基础关联分析、标准脆弱性管理、风险评估、首页、标准的报表模块、标准的响应管理模块、权限管理、知识管理、系统自身管理、内置 1 个本地事件采集器，默认支持不低于 30 管理节点授权。 3、系统必须采用 B/S 架构，管理员只需浏览器即可连接到系统进行各种操作。用户的浏览器客户端无需安装 JRE 或者 JAVA Web Start 即可访问管理中心。产品要求集成数据库，无须再独立安装数据库系统，亦无须对数据库进行专门的维护。 4、系统具有资产管理的功能，能够将被管理 IT 资产进行分组、分域的统一维护。系统提供基于资产的拓扑视图，可以显示资产之间的逻辑连接关系。系统可以按列表和拓扑两种模式显示资产拓扑节点。 5、无需另外安装软件组件，管理中心即可通过 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC 等多种方式完成日志收集功能。 6、系统允许管理员实时的，以实时监视策略的形式从各个维度查看安全事件。可以对选中的事件源/目的 IP 地址进行全球地图定位，包括在线定位和离线定位。可以对选中的事件进行事件拓扑分析，并可视化的展示一幅描述事件之间相互关系的事件拓扑图。 7、系统具有基于规则的安全事件实时关联分析的能力，能够对不同的事件进行相关性分析，发掘潜在的信息。系统提供基于图形化方式的关联规则编辑器。 8、关联分析规则具备测试功能，分析师能够更方便地对新设计的关联规则进行模拟测试，以便调校规则的作用效果，支持《一种多维度网络态势感知的方法、设备及系统》相关技术，提供证明材料。 9、系统具有弱点管理功能，能够导入资产的弱点信息，并计算资产/安全域/业务系统的脆弱性值。系统通过内置的风险计算模型，综合考虑资产的价值、脆弱性和威胁，计算风险的可能性和风险的影响性。 10、告警动作支持告警重定义、弹出提示框、播放警示音、发送邮件、

			发送 SNMP Trap、发送短信、执行命令脚本、设备联动、发送飞鸽传书、发送 Syslog、设置观察列表等方式。
5		管理区网络集中管理平台	1、产品能够部署在 Windows 和 Linux 操作系统上，具备自主知识产权的通用软件平台，具备高可靠高扩展性等特点。 2、内置数据库，包即包含系统平台框架、资产管理、安全事件管理、基础关联分析、标准脆弱性管理、风险评估、首页、标准的报表模块、标准的响应管理模块、权限管理、知识管理、系统自身管理、内置 1 个本地事件采集器，默认支持 30 管理节点授权。 3、系统必须采用 B/S 架构，管理员只需浏览器即可连接到系统进行各种操作。用户的浏览器客户端无需安装 JRE 或者 JAVA Web Start 即可访问管理中心。产品要求集成数据库，无须再独立安装数据库系统，亦无须对数据库进行专门的维护。 4、系统具有资产管理的功能，能够将被管理 IT 资产进行分组、分域的统一维护。系统提供基于资产的拓扑视图，可以显示资产之间的逻辑连接关系。系统可以按列表和拓扑两种模式显示资产拓扑节点。 5、无需另外安装软件组件，管理中心即可通过 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC 等多种方式完成日志收集功能。 6、系统允许管理员实时的，以实时监视策略的形式从各个维度查看安全事件。可以对选中的事件源/目的 IP 地址进行全球地图定位，包括在线定位和离线定位。可以对选中的事件进行事件拓扑分析，并可视化的展示一幅描述事件之间相互关系的事件拓扑图。 7、系统具有基于规则的安全事件实时关联分析的能力，能够对不同的事件进行相关性分析，发掘潜在的信息。系统提供基于图形化方式的关联规则编辑器。 8、关联分析规则具备测试功能，分析师能够更方便地对新设计的关联规则进行模拟测试，以便调校规则的作用效果，支持《一种多维度网络态势感知的方法、设备及系统》相关技术，提供证明材料。 9、系统具有弱点管理功能，能够导入资产的弱点信息，并计算资产/

			安全域/业务系统的脆弱性值。系统通过内置的风险计算模型，综合考虑资产的价值、脆弱性和威胁，计算风险的可能性和风险的影响性。 10、告警动作支持告警重定义、弹出提示框、播放警示音、发送邮件、发送 SNMP Trap、发送短信、执行命令脚本、设备联动、发送飞鸽传书、发送 Syslog、设置观察列表等方式。
6		销售区网络集中管理平台	1、系统功能：负责全省投注站 3000 多个安全接入终端及相关设备的准入控制，以及管理、维护、状态展示、报表生成等。 2、终端设备管理：支持对投注站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投注站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：支持投注站安全接入终端设备的远程登陆、故障排查；支持投注站安全接入终端设备的远程升级；支持投注站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：支持投注站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；支持投注站安全接入终端设备的外网接入、投注机接入、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。
7		运行平台	★①主运行平台：1 套，提供基于 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。②存储服务器：2 台，配置不低于 I3-8100 处理器，16G 内存，1T 硬盘，2 个千兆电口。
8		定制开发	①定制投注站终端的统一运维管理：安全接入终端是投注站的核心接入设备，关联着投注机、电子走势图、视频监控以及辅助投注设备，是投注站的运维和管理重点，该系统需与现有的站点综合安全接入系统无缝兼容和联动，并实现全省数千个站点的安全接入终端、上万个各类售彩设备、辅助售彩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。 ②销售区集中管理平台定制开发：投注站有全国统一的双色球、3D，也有地方性快开游戏等，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站点综合安全接入平台定制开发：安全接入终端是投注站的核心接入设备，也是投注站数据交换的枢纽，各类销售终端均与其相连。需要与行业统一安全认证系统、行业聚合支付应用系统、站点综合安全接入系统等无缝对接，实现站点投注机等各类售彩设备统一的“安全通讯、安全认证和安全支付”和统一管理要求。建立起投注站各类销售终端的准入控制和安全管理机制，以利于整体防控。 ★以上①②③项供应商需要提供定制开发承诺函，并承诺在合同签订后 30 日内完成，符合甲方或指派第三方项目验收条件。
9	CA 数字证书认证平台	CA 数字证书认证系统	①管理功能: 提供基于 WEB 的管理员界面，基于 https 访问，管理员基于用户名密码认证。提供管理 API，方便与其他系统集成。 ②业务系统管理功能: 提供业务系统管理，可以创建、修改和删除业务系统。支持为每个业务系统建立系统身份 ID，包括但不局限于以下系统： ✓ 社会化渠道管理系统

			✓ 彩票游戏热线系统 ✓ 综合业务安全接入系统 ✓ 电子支付系统 ✓ ... ③业务系统服务器白名单管理: 提供基于业务系统服务器的 ID 和 IP 的白名单管理服务，如果服务器的 ID 和 IP 不在指定的白名单中，不允许认证通过，并提供审计日志。 ④终端黑名单管理: 提供基于终端 KEYID 和设备 ID 的黑名单管理，如果终端的 KEYID 或者设备 ID 位于黑名单中，则阻止该终端对认证平台的访问，并记录日志。 ⑤审计管理: 提供基于业务的数据审计管理，记录终端对认证平台的注册、和业务系统的身份认证，投注订单的签名。 当发生了已成交易或者异常认证事件之后，可以通过该平台的审计信息进行事件调查。 ⑥统计与报表: 提供完善的统计和报表功能，对认证平台的访问进行监控。 基于时间的访问量监控。 基于业务的访问量统计。 基于服务器的访问统计与监控。 基于终端的访问统计。 ⑦异常访问监控 可以设置安全阈值，当某个业务系统对认证平台的访问超过设定阈值后，就会生成异常访问日志，如单个投注终端单日访问量超过一定的阈值。 ⑧短信告警功能 当发生系统异常的情况后，通过短信方式提醒管理员。 ⑨日志功能

			系统本身的日志功能，记录管理员登录，以及系统功能的修改。
10		运行平台	①加密机： 数量 2 台。 ★产品形态为 2U 机架式设备，冗余电源，前面板需提供 4 个 10/100/1000M 自适应 RJ45 以太网接口；1 个管理网口；1 个控制串口；4 个 USB 端口；前面板需提供控制口 RJ45 口 1 个，并配有专用串口线，可通过控制口对密码机进行维护管理。 具备国家密码管理局颁发的有效的《商用密码产品型号证书》，全面支持 SM1、SM2、SM3、SM4 等国家商用密码算法。 采用国家密码管理局许可的密码算法芯片实现 SM1、SM2 等密码算法，保证算法实现的安全性和高效性。 采用专用的安全硬件进行内部密钥和敏感信息的存储，支持紧急情况下快速数据销毁功能，包括开盖自动毁钥和手动毁钥两种方式。 设备前面板应具备主动毁钥按钮，可进行手动毁钥操作。 具备“系统保护密钥-用户密钥（SM2 密钥对和密钥加密密钥）-会话密钥”的三层密钥保护结构，保证用户密钥及应用系统的安全性。 采用多路国家密码管理局许可的物理噪声源芯片并行生成随机数，异或后输出使用，保证随机数的生成质量。 ②USB KEY：数量：10 个。 ★符合中福彩安全认证平台要求，提供承诺函并加盖公章。 SM1 加解密速度：不低于 100Kbps。 SM2 签名验签：不低于 20 次/秒。 SM3Hash 运算速率：不低于 20Mbps。 ③数据运算与存储： 数量：6 台。 机架式服务器，不低于 2U 高度，配置不低于：英特尔至强 E5-2620V4，内存≥32G，硬盘≥2T，硬盘类型：SAS，磁盘陈列卡：H730-1G 缓存，光驱：DVDRW*1，750W 双电源，导轨*1。

			★中标方应有满足如期交货的能力保障并做出承诺，若无法在规定的时间内交付货物（合同签订后的 15 个工作日），提供承诺函并加盖公章。
11		定制开发	1、业务功能模块定制开发要求： ①基础数据服务模块： 对中心数据进行统一规划和设计，实现中心内部以及与市中心间数据的集中处理、交换和管理，并通过统一接口对上层应用提供准确、全面的数据服务，逐步形成规范的数据共享支撑中心二、身份认证模块。 ②开发框架服务模块： 统一各类基础应用的开发框架及接口标准，支持多种服务接口和灵活扩展。每种公共服务采用开放轻量 API 接口，支持各类应用（包括第三方应用）重用服务模块进行业务创新。 ③应用集成服务模块： 为中心内、外部应用集成提供接口（如认证、加密、权限控制和双活运营模式、数据备份等），使不同的云应用和上层业务应用灵活调用下层服务，保证数据在系统间实时交换、统一呈报。 2、密码机主要指令适配定制开发要求： ①遵循 GM/T 0018-2012《密码设备应用接口规范》适配开发，并提供标准的国密 SDF 接口。 ②密码机需适配支持以下主要指令： 产生 SM2 密钥对并使用内部密钥加密输出：产生 SM2 密钥对并输出，其中私钥使用指定索引的内部 SM2 密钥加密后输出； 产生 SM2 密钥对并使用外部公钥加密输出：产生 SM2 密钥对并输出，其中私钥使用外部指定的 SM2 公钥加密后输出； 产生 SM2 密钥对并使用对称加密输出：产生 SM2 密钥对并输出，其中私钥使用指定索引的对称密钥加密后输出； SM2 私钥转保护 1：将由内部 SM2 密钥加密保护的私钥转换为外部指定的 SM2 公钥加密保护；

			SM2 私钥转保护 2：将由内部对称密钥加密保护的私钥转换为外部指定的 SM2 公钥加密保护； 导出 SM2 密钥对：导出指定索引的 SM2 密钥公私钥对使用，其中私钥使用外部指定的 SM2 公钥加密后输出； 导出对称密钥：导出指定索引的对称密钥，该对称密钥使用外部指定的 SM2 公钥加密后输出； 导出 SM2 公钥：导出指定索引的 SM2 密钥对的公钥，支持同时导出签名和加密公钥； SM2 私钥转保护：将内部 ECC 公钥保护的私钥数据装换成外部 ECC 公钥保护的私钥密文数据； 单包杂凑运算：计算输入数据的 SM3 杂凑值； 单包对称加密：使用外部指定对称密钥对明文进行 SM1/SM4 加密，支持 PKCS#5 填充模式； 单包对称解密：使用外部指定对称密钥对密文进行 SM1/SM4 解密，支持 PKCS#5 填充模式； 生成 SM2 数据签名：对待签名数据进行预处理，并计算 SM2 签名值； 验证 SM2 数据签名：对待验签数据进行预处理，并验证 SM2 签名值； 导出 SM2 公钥：导出指定索引的 SM2 密钥对的公钥，支持同时导出签名和加密公钥； 导入 SM2 加密密钥对：使用指定索引的签名私钥解密数字信封，得到加密密钥对私钥，并保存加密密钥对到指定索引位置； 批量导入 SM2 加密密钥对：依次使用设备密钥加密私钥对数字信封进行解封，并保存加密密钥对到指定索引位置； 导入对称密钥：使用指定索引的 SM2 私钥解密出对称密钥，并将该对称密钥保存在指定索引的对称密钥空间； 认证数据转换：使用认证服务系统的加密私钥解密出随机数 Ra；生成随机数 Rb；使用终端的加密公钥加密 Ra||Rb 得到认证数据密文； 密钥数字信封封装：生成指定长度密钥，并使用基于 SM2 算法的数字

			信封封装后输出； 密钥数字信封解封：对基于 SM2 算法的数字信封进行解封得到明文密钥。 ③需要根据中福彩认证系统的实际情况不断完善，以满足行业建设要求。 ★以上 1、2 项供应商需要提供定制开发承诺函，并承诺在合同签订后 30 日内完成，符合甲方或指派第三方项目验收条件。 **▲CA 数字证书认证平台是网络安全建设的核心，需要与中福彩 CA 安全认证系统对接才能实现新业务推广，供应商必须在规定时间完成定制开发并提供承诺函，对夸大或响应不实者，用户有权终止项目并追究责任。**

3.1.3、销售网络通用安全产品技术指标要求

序号	名称		技术要求
1	下一代防火墙	产品配置	1、系统要求： 具有下一代防火墙的基本功能。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： 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；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、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，提供界面截图并加盖厂商公章。 ★5、配置不低于：2U 机架式设备，配置冗余双电源，电口支持硬件 BYPASS；不少于 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。
		数量	9 台。
		服务	★标配 IPS、防病毒模块，提供原厂商三年产品质保服务，三年入侵特征升级库服务，三年病毒特征库服务，提供原厂商服务承诺函。
2	入侵防御系统	产品配置	1、入侵防御功能：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 种以上网络协议，并支持至少 7 种以上弱口令检测元素，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。 4、病毒防御功能： 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。 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。 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。 5、恶意代码检测功能： 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。 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。 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。 ★6、配置不低于：2U 硬件平台，配置冗余双电源，电口需支持硬件 BYPASS；不少于 6 个 10/100/1000 Base-T 接口，不少于 4 个扩展槽位，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。
		数量	4 台。
		服务	★标配防病毒模块。提供原厂商三年产品质保服务，三年入侵特征升级库服务，三年病毒特征库服务，提供原厂商服务承诺函。
3	WEB 应用防火墙	产品配置	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、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、支持透明、代理模式、旁路部署、单臂部署、策略路由部署。 ★5、2U 机架式设备，不少于 4*1000BASE-T，1*RS232，可根据需求进行扩展。HTTP 请求/秒:不低于 20,000，TCP 并发连接: 不低于 2,000,000；单接口吞吐量(Mbps):不低于 1000M，整机吞吐量(Gbps):

			不低于 4G。
		数量	1 台。
		服务	★提供原厂商三年产品质保服务，提供原厂商服务承诺函。
4	数据库审计	产品配置	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、运行状态等信息监视功能；提供审计策略和配置的导入导出。 ★5、标准 1U 机架式设备，不少于 6 个千兆电口，至少具备 4 个业务口、1 个带外管理口、1 个 HA 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。审计数据库数量不低于 5 个。

		数量	1 台。
		服务	★提供原厂商三年产品质保服务，提供原厂商服务承诺函。
5	上网行为管理系统	产品配置	1、支持路由模式、透明（网桥）模式、混合模式，支持镜像接口，部署模式切换无需重启设备。 2、支持 4G 网络，在主线路出现问题时，自动切换到 4G 网络，保障网络正常运行。 3、支持服务器负载均衡，支持一个公网 IP 映射到内网多台服务器，服务器间支持连接和源地址 hash,支持服务器健康检查。 4、支持通知页面推送功能，支持向 PC 端浏览器 4 个方位推送，手机端支持全屏推送。 5、内网资产监控，可对终端风险级别、操作系统、浏览器类型、应用、杀毒软件等方面进行监控。 6、上网行为管理应对文件的下载有深入控制能力。 7、要求提供具备细化网络服务控制、系统及代理 MSN 服务器的能力证明。 ★8、1U 机箱，4 个 Combo 千兆接口，10 个 10M/100M/1000M 自适应电口，Bypass 接口 1 对；整机吞吐量不小于 4Gps，最大并发连接数不小于 200 万，支持接入带宽不小于 150M；500G 存储空间；支持最大用户数不小于 1500 人；支持软硬件 Bypass，设备断电或出现故障时保障业务链路的正常运行。
		数量	1 台。
		服务	★提供原厂商三年产品质保服务，提供原厂商服务承诺函。
6	漏洞扫描系统	产品配置	★1、1U 机架式设备，标配 6 个电口，1 个接口扩展插槽；2 个 USB 接口、1T 以上 SATA 硬盘。单任务可扫描 100 个 IP 地址，具体 IP 地址不限。 2、支持对扫描的任务报告进行合并，合并数量不限，合并过的报告还可以再次进行合并操作。 3、扫描对象应支持服务器、客户机、网络打印机等；操作系统应支持 Microsoft Windows 9X/NT/2000/XP/2003/Vista/2008/7、Sun Solaris、

			HP Unix、IBM AIX、IRIX、Linux、BSD 等；网络设备应支持 Cisco、3Com、Checkpoint、华为、Alcatel 等主流网络设备；应用系统应支持数据库（SQL Server、Oracle、Sybase、DB2、MySQL）、Web、FTP、电子邮件等。 4、支持扫描常见的应用软件漏洞，包括 IE 浏览器、MSN、Mozilla Firefox、Yahoo Messenger、MS Office、多媒体播放器（如 Media Player）、VMware 虚拟机和 P2P 客户端软件（如 BitTorrent 客户端等）的安全漏洞；漏洞扫描方法应不少于 70000 种；支持扩展 Web 应用扫描、基线核查功能 漏洞库与 CVE、CNCVE、CNNVD 和 BUGTRAQ 等国际、国内标准兼容。支持扫描 IPv6 环境中的设备、系统。 5、支持云平台扫描，漏洞覆盖 OpenStack 、KVM、Vmware、Xen 等主流的云计算平台（截图证明，加盖厂商公章）。 6、支持对 Apple 软件和应用进行扫描，含 MAC OS，Safari，itunes 等。
		数量	1 套。
		服务	★提供原厂商三年硬件质保与特征库升级，提供原厂商服务承诺函。
7	堡垒机	产品配置	★1、标准 1U 设备，标配不少于 6 个千兆电口，一个扩展插槽,1 个 console 管理口。字符协议不低于 700 个，图形协议不低于 200 个，硬盘容量不小于 1TB；支持最大管理授权数不小于 500 个，本次配置授权数 50 个。 2、字符协议：SSHv1、SSHv2、TELNET、RLOGIN、TN5250（AS400）；图形协议：RDP、VNC；文件传输协议：FTP、SFTP；数据库协议：支持 Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL 等数据库类型。 3、Windows 类主机、Unix 类主机、Linux 类主机、主流网络设备。 4、支持通过堡垒机 web 页面内嵌 Ssh、Ftp、Telnet、Rdp\Vnc 运维工具访问目标资源。 5、针对 SSH、Telnet、Rlogin、FTP/SFTP、数据库操作进行记录及审

			计；记录会话时间、命令执行时间、会话协议、服务端 IP、服务器端口、客户端 IP、客户端端口、操作命令、返回信息、运维用户帐号、审批用户帐号、资源账号等信息； 6、针对 RDP、VNC 等图形终端操作的连接情况进行记录及审计；记录会话时间、命令执行时间、录像文件名等信息； 7、按设备（设备组）、系统帐号、计划开始时间、改密周期、密码策略、改密结果发送等信息配置改密计划，到期自动执行； 随机生成不同密码、随机生成相同密码以及手工指定相同密码的密码策略，并严格遵守密码强度设置，支持手工改密功能。 8、自动改密支持 Linux、Unix、Windows、AIX 以及 Oracle、SqlServer、PostgreSQL、MySql、DB2、Informix 、SYBASE 的内置自身账号密码 ★9、支持多重冗余协议(MRP)，实现链路备份、端口冗余、双机热备份、集群备份等（提供证明文件，加盖厂商公章）
		数量	1 台。
		服务	★提供原厂商三年产品质保服务，提供原厂商服务承诺函。
8	网络准入控制系统	产品配置	★1、标准 1U 设备，标置 6 个千兆电口，包含管理口和 HA 口；可扩 4 个 1000M 光口或 4 个 1000M 电口。每秒事务数（TPS)不小于 1700（次/秒），最大吞吐量不小于 800Mbps，最大支持 800 个终端设备和 800 个认证用户；含 100 用户授权。 2、支持双操作系统冷备，当常用系统出现故障，可以使用备用系统恢复（截图证明，加盖厂商公章）。 3、准入设备支持透明网桥方式的准入技术，并支持 Bypass；准入设备必须支持多种准入技术的复用，到少四种以上，如 802.1x、DHCP、策略路由混合部署。 4、支持终端入网的安全基线检查、软件安全检查、账户密码安全检查、环境安全检查等检查项； 5、支持当前主流智能终端设备的安全准入控制；能够提供移动终端入网的设备注册功能；实时监测哑终端指纹信息的变化，当哑终端指纹信息变化时，可及时对其进行告警或阻断。

			6、支持针对网络流量的识别功能，发现资产及连接关系、通信协议、应用层访问指令等，并可以根据学习信息辅助生成安全访问控制规则。 7、支持摄像头、门禁、网络打印机、叫号机、自助查询机等各类业务终端资产的行为画像（截图证明，加盖厂商公章）。 8、支持根据行为模型的安全接入机制，可根据终端日常业务行为自动生成终端行为基线 ；自动判断网络中哑终端的异常行为及偏离程度，并对风险进行告警或阻断。
		数量	1 台。
		服务	★提供原厂商三年产品质保服务，提供原厂商服务承诺函。
9	防病毒系统	产品配置	★1、PC 端授权：120 点，服务器端授权：80 点。 2、能够对已知、未知病毒、木马、恶意程序等进行检测、清除。能够对各种加壳的病毒文件进行病毒查杀，支持的加壳种类不少于 100 种。 3、能够实时监控和清除病毒、木马、恶意程序等，杀毒软件须提供宏病毒专杀引擎，可以解析办公软件所有常用版本的文档，处理被感染的文档，将恶意代码清除而保留正常文档。清除操作的粒度可以到清除 excel 公式、宏脚本中某个函数等。 4、具备压缩包查杀功能，支持 25 种解压缩格式，涵盖压缩包、安装包、文档格式解析能力。支持安装脚本级查杀，拦截流氓软件捆绑。 5、具备系统文件监控能力，能够监控计算机系统所有活跃文件的安全性 具备边界防护能力，对网页访问、浏览器下载、U 盘拷贝等系统入口实时监控，拦截危险文件的落地。
		数量	1 套。
		服务	★提供原厂商提供三年产品质保及技术支持服务，三年病毒特征库服务。提供原厂商服务承诺函。
10	综合日志审计系统	产品配置	★1、1U 标准机架式设备，采用专用安全操作系统；系统具有 6 个千兆日志采集口，支持 Console 口管理；系统有效存储容量不少于 2TB；支持 30 个审计对象授权。 2、系统必须采用基于浏览器的用户界面，为了适应不同用途，用户可

			以对界面颜色进行选择调整（截图证明，加盖厂商公章）； 3、能对网络设备、安全设备和系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警等安全信息进行全面的审计； 4、无需另外安装软件组件，审计中心即可通过 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFPT、NetBIOS、OPSEC 等多种方式完成日志收集功能；针对文本格式的日志采集，支持本地文件、Windows 共享和 FTP、SFTP 获取四种采集方式； 5、可以对选中日志进行视网膜视图分析，以可视化方式展示日志的源 IP 与目的 IP 分布走向；系统允许管理员以统计场景的形式查看不同类型的日志信息；用户可自定义统计场景，每个统计场景都要以统计策略的形式进行存储，并形成一个统计树。 6、系统提供基于图形化方式的规则编辑器；可以针对事件属性引用规则、应用资产属性、引用资源；可实现统计计数关联，能够设定一段时间内的事件发生次数的阈值，还能指定重复事件的属性特征。 7、根据关联分析的结果将可疑或者需要关注的信息加入观察列表，并可以对观察列表中的信息进行关联，也可以被任何规则引用。 8、告警内容可以自定义，可以根据日志的实际情况将参数传递给命令行脚本；内置颜色库，可以对不同告警等级设置不同的颜色标识；系统采用基于策略的日志分析模式，使用户从传统的“条件编辑”式的分析体验转变为“策略选取”式的分析体验；系统内置超过 3000 条分析策略，包括各种实时分析策略、历史分析策略、告警统计策略、仪表板视图。
		数量	4 台
		服务	★提供原厂商三年产品质保服务，提供原厂商服务承诺函。

3.2、核心业务区综合安全防控服务

序号	名称		技术要求
1	核心业务区综合安全防控服务	主要服务内容	1、服务期内，为核心业务区提供“一站式”综合安全托管服务，包括必要的安全设备、防护措施和安全服务，并满足等级保护 2.0 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综合防控： ①电脑票销售系统； ②即开票销售系统； ★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。投标人需要提供承诺函。
2		主要防护措施	1、服务期内，利用基础安全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大数据安全分析平台； ②网络集中管理平台； ③CA 数字证书认证平台； 2、服务期内，利用通用安全设备为核心业务区提供综合安全防护服务，包括但不局限于以下安全设备： 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：包括但不局限于下一代防火墙、入侵防御系统、WEB 应用防火墙、数据库审计系统、上网行为管理系统、漏洞扫描系统、堡垒机、网络准入控制系统、防病毒、日志审计系统等； 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安全设备升级维护服务 ②安全评估渗透测试服务 ③定期巡检安全检查服务 ④安全漏洞定期通报服务 ⑤紧急事件安全应急服务 ⑥重大事件安全值守服务 ⑦等级保护业务指导服务 ⑧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级保护 2.0 要求、整改意见、安全域划分以及行业应用要求提出建设方案，并为核心业务区提供“一站式”综合防控服务，投标人需要提供承诺函。

3.3、支撑业务区综合安全防控服务

序号	名称		技术要求
1	支撑业务区综合安全防控服务	主要服务内容	1、服务期内，为支撑业务区提供“一站式”综合安全托管服务，包括必要的安全设备、防护措施和安全服务，并满足等级保护 2.0 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业务系统综合防控： ①中福彩中心接入区； ②市福彩中心接入区； ③传统投注站接入区； ★3、随着行业应用系统不断地增加，在服务期内，支撑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。**投标人需要提供承诺函。**

2		主要防护措施	1、服务期内，利用基础安全平台为支撑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大数据安全分析平台； ②网络集中管理平台； ③CA 数字证书认证平台； 2、服务期内，利用通用安全设备为支撑业务区提供综合安全防护服务，包括但不局限于以下安全设备： 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：包括但不局限于下一代防火墙、入侵防御系统、WEB 应用防火墙、数据库审计系统、上网行为管理系统、漏洞扫描系统、堡垒机、网络准入控制系统、防病毒、日志审计系统等； 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安全设备升级维护服务 ②安全评估渗透测试服务 ③定期巡检安全检查服务 ④安全漏洞定期通报服务 ⑤紧急事件安全应急服务 ⑥重大事件安全值守服务 ⑦等级保护业务指导服务 ⑧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级保护 2.0 要求、整改意见、安全域划分以及行业应用要求提出建设方案，并为支撑业务区提供“一站式”综合防控服务，**投标人需要提供承诺函。**

3.4、外联业务区综合安全防控服务

序号	名称		技术要求
1	外联业务区综合安全防控服务	主要服务内容	1、服务期内，为外联业务区提供“一站式”综合安全托管服务，包括必要的安全设备、防护措施和安全服务，并满足等级保护 2.0 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电信运营商等接入区； ②农业、兴业、中行等银行接入区； ③渠道商等外联单位接入区； ★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。投标人需要提供承诺函。
2		主要防护措施	1、服务期内，利用基础安全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大数据安全分析平台； ②网络集中管理平台； ③CA 数字证书认证平台； 2、服务期内，利用通用安全设备为外联业务区提供综合安全防护服务，包括但不局限于以下安全设备： 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：包括但不局限于下一代防火墙、入侵防御系统、WEB 应用防火墙、数据库审计系统、上网行为管理系统、漏洞扫描系统、堡垒机、网络准入控制系统、防病毒、日志审计系统等；

			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安全设备升级维护服务 ②安全评估渗透测试服务 ③定期巡检安全检查服务 ④安全漏洞定期通报服务 ⑤紧急事件安全应急服务 ⑥重大事件安全值守服务 ⑦等级保护业务指导服务 ⑧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级保护 2.0 要求、整改意见、安全域划分以及行业应用要求提出建设方案，并为外联业务区提供“一站式”综合防控服务，投标人需要提供承诺函。

3.5、外部办公区综合安全防控服务

序号	名称		技术要求
1	外部办公区综合安全防控服务	主要服务内容	1、服务期内，为外部办公区提供“一站式”综合安全托管服务，包括必要的安全设备、防护措施和安全服务，并满足新的等级保护制度（等级保护 2.0）建设要求和行业安全建设要求。 2、外部办公区安全防控包括但不局限于以下接入管理： ①办公服务区； ②官网官微服务区； ③运营管理区； ★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。投标人需要提供承诺函。

2		主要防护措施	1、服务期内，利用基础安全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大数据安全分析平台； ②网络集中管理平台； ③CA 数字证书认证平台； 2、服务期内，利用通用安全设备为外部办公区提供综合安全防护服务，包括但不局限于以下安全设备： 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：包括但不局限于下一代防火墙、入侵防御系统、WEB 应用防火墙、数据库审计系统、上网行为管理系统、漏洞扫描系统、堡垒机、网络准入控制系统、防病毒、日志审计系统等； 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安全设备升级维护服务 ②安全评估渗透测试服务 ③定期巡检安全检查服务 ④安全漏洞定期通报服务 ⑤紧急事件安全应急服务 ⑥重大事件安全值守服务 ⑦等级保护业务指导服务 ⑧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级保护 2.0 要求、整改意见、安全域划分以及行业应用要求提出建设方案，并为外部办公区提供“一站式”综合防控服务，投标人需要提供承诺函。

3.6、网络安全专项安全服务

序号	名称		技术要求
1	网络安全专项安全服务	主要服务内容	1、服务期内，提供针对销售网络展开的专项安全服务，服务期间的相关设备、人员和服务由服务商提供。 2、专项安全服务包括但不局限于以下服务内容： ①协助进行等级保护的测评、整改、自查工作； ②在相关部门展开专项攻防演练时提供安全服务； ③服务期内的安全巡检，应急响应和驻场服务； ★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，以满足等级保护及行业的安全建设要求。供应商需要提供承诺函。
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，协助进行等级保护的测评、整改、自查工作，并且协助完成电脑票系统、即开票系统、运营管理系统、官网管微系统、综合营销管理系统的定级、备案工作，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前，供应商需要按照等级保护测评的标准进行自查，并提出整改建议和完善方案，供应商提供承诺函； 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，并满足等级保护相关的要求，供应商提供承诺函； ③进行等级保护的巡检工作时，供应商需要按照等级保护测评的标准和要求进行巡检工作，供应商提供承诺函。 2、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类、应用类安全评估工具、攻防演练工具等，供应商提供承诺函； ②人员包括但不局限于以下要求：提供不少于三人的安全服务

			专家团队，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。 3、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：中心机房月度安全巡检、站点季度安全巡检等，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标准化服务：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。 ⑤本地化服务：集中服务期，提供本地化服务人员不少于 3 人，日常工作期，提供驻场服务人员不少于 1 人； ★4、以上具体服务内容依据等级保护 2.0 要求、整改意见、行

			业应用要求和省中心实际情况提供安全服务方案和服务内容，供应商需要提供承诺函。

第五章 电子响应文件组成

一、协商响应声明

致 _____(采购人)：

根据贵方为_____(项目名称)的协商邀请（采购文件编号：_____），签字代表（全名、职务）经正式授权并代表_____

（供应商名称）提交固化的电子响应文件（含其对应的哈希值）1 份。

一、我方同意在本项目单一来源采购文件中规定的递交响应文件截止时间起__天内(电子响应文件有效期)遵守本电子响应文件中的承诺且在此期限期满之前均具有约束力。

二、我方承诺（承诺期：成立三年以上的，为提交响应文件截止时间前三年内；成立不足三年的，为实际时间）：

（一）我方依法缴纳了各项税费及各项社会保障资金，没有偷税、漏税及欠缴行为。

（二）我方在经营活动中没有存在下列重大违法记录：

1.受到刑事处罚；

2.受到三万元以上的罚款、责令停产停业、在一至三年内禁止参加政府采购活动、暂扣或者吊销许可证、暂扣或者吊销执照的行政处罚。

三、我方已详细审核全部单一来源采购文件，包括单一来源采购文件修改文件（如有的话）、参考资料及有关附件，确认无误。我方承诺接受单一来源采购文件中的全部条款且无任何异议。

四、我方保证响应文件提供的数据和材料是真实、准确的。我方愿意向贵方提供任何与本项采购有关的数据、情况和技术资料。若贵方需要，我方愿意提供我方作出的一切承诺的证明材料。

五、我方承诺遵守《中华人民共和国政府采购法》的有关规定，保证在获得成交资格后，按照单一来源采购文件确定的事项签订政府采购合同，履行双方所签订的合同，并承担合同规定的责任和义务。

供应商(公章)：

法定代表人或委托代理人(签字)：

日　　期：年 月 日

附件1

法定代表人身份证明(法定代表人参加协商)

供应商名称：_____

注册号：_____

注册地址：_____

成立时间：_____年 _____月____ 日

经营期限：_____

经营范围：主营：_____ ；兼营：_____

姓名：_____ 性别：_____ 年龄：_____ 系_____（投标人名称）的法定代表人。

特此证明。

法定代表人身份证 **原件扫描件（正反面）**

供应商（公章）：

法定代表人（签字）：

日　　期：_____年____月____日

附件 2

法定代表人授权书(委托代理人参加协商)

_____（采购人名称）：

本授权声明：_____（供应商名称）_____（法定代表人姓名、职务）授权_____（被授权人姓名、职务）为我方“_____”项目（单一来源采购文件编号）采购活动的合法代表，以我方名义全权处理该项目有关报价、签订合同以及执行合同等一切事宜。

特此声明。

法定代表人身份证 **原件扫描件（正反面）**	**委托代理人身份证** **原件扫描件（正反面）**

投标人（公章）：

法定代表人（签字）：

委托代理人（签字）：

日　　期：_____年____月____日

二、商务/响应性方案

（一）商务偏离表

项目名称：

采购文件编号：

序号	包号	采购文件要求	响应情况	偏离情况	说明

供应商（公章）：

法定代表人或委托代理人（签字）：

日　　期：　年　　月　日

说明：1.“偏离情况”系指“正偏离”、“负偏离”或“无偏离”。

2. 请逐条对应采购文件的“商务要求”和“合同条款”中要求（若有）的商务要求，认真填写该表。

3. “说明”系指供应商提供的证明材料类型、证明材料与技术规格相对应的页码及条款号。不按要求填写“证明材料说明”或提供虚假材料的，采购小组有权判定该响应文件无效。

（二）技术规格偏离表

项目名称：

采购文件编号：　　包号：

序号	包号	采购名称（内容）	采购文件要求	响应情况	偏离情况	说明

供应商（盖章）：

法定代表人或委托代理人（签字）：

日　　期：　　年　　月　　日

说明：1.“偏离情况”系指“正偏离”、“负偏离”或“无偏离”。

2.请按响应产品的实际技术参数，逐条对应采购文件“第四章”中的采购需求要求认真填写该表。该表不能作为响应产品的技术文件，供应商应在响应文件中单独提供技术文件。

3.“说明”系指供应商提供的证明材料类型、证明材料与技术规格相对应的页码及条款号。不按要求填写“证明材料说明”或提供虚假材料的，采购小组有权判定该响应文件无效。

三、供应商响应方案（或内容）

注：格式自拟

四、服务方案及服务承诺书

注：格式自拟

五、报价一览表

供应商名称：

项目名称：

采购文件编号：　　包号：

币种：人民币

报价	大写：_____ 小写：_____
采购内容	
项目负责人	
备　注	

供应商（盖章）：

法定代表人或委托代理人（签字）：

日　　期：　　年　　月　　日

说明：1. 投标总价应是最终用户验收合格后的总价，包括设采购文件招标内容所涵盖和规定的全部费用。

2.“报价一览表”为多页的，每页均需由法定代表人或委托代理人签字并盖供应商印章，否则为无效响应。

3、“报价一览表”以包为单位填写。

六、报价明细表

注：格式自拟

供应商（盖章）：

法定代表人或委托代理人（签字）：

日　　期：　　年　　月　　日

七、供应商认为需要提供的其它资料

第六章　政府采购项目供应商满意度问卷

项目名称：

采购文件编号：

1、您对集采机构在本次项目中工作人员服务态度和质量是否满意？

A.满意（） B.不满意（）

2、请为集采机构本次政府采购代理的服务态度和质量评分

A.优（） B.良（） C.一般（） D.差（）

（选择“一般”及“差”答案时须填写理由以方便改进）：

3、您认为集采机构哪些方面还需要进行改进？

A.没有意见（）

B.（详细意见或建议）：

供应商（盖章）：

法定代表人或委托代理人（签字）：

日　　期：　　年　　月　　日

说明：本表格由供应商填写，请在相应的括号打“√”。**自成交公示发布之日起7个工作日内递交给集采机构。**

附件 1

“甘肃省公共资源交易局网上开标系统”
投标供应商用户手册

1. 准备工作

准备一台携有摄像头及耳麦的电脑，操作系统建议采用 windows7 以上版本，浏览器建议采用 360 安全浏览器，安装钉钉、办公软件（wps 或 office）。

2. 系统登录

网上开评标系统，投标人有两种登录方式：①账号+密码+验证码；②证书+密码+pin 码

说明：①登录账号是在甘肃省公共资源交易主体共享平台注册的账号（11 位手机号码），密码是对应设置的密码。

②证书登录的前提是对应的证书必须在甘肃省公共资源交易主体共享平台做过 CA 互认（绑定）的锁。（文锐、成兴、江苏翔晟、国泰新点、交易通、金润）

用户注册、用户查询、密码重置、**CA 互认的操作请全部详见《CA 互认操作手册》。**

甘肃省公共资源主体共享平台的链接地址 ：

http://ggzyjy.gansu.gov.cn/f/shuzikey/web.html

选择角色，登录系统。

3. 我要投标

找到要参加的项目，如图提示操作。

说明：确认投标标段时，切记要一次性勾选全部要参与的标段，不可分批次操作，请谨慎操作。

确认投标-“进入网上开标厅”

下载成功。

4. 固化电子投标文件

下载并安装电子投标文件固化工具，并完成电子投标文件的固化（具体操作参见《电子投标文件固化工具用户手册》）。

5. 上传哈希值（hash）

复制哈希值的方法有两种：①可在电子投标文件固化导出之后的界面直接复制；②在固化导出后的文件夹路径下，打开 txt 文档进行复制。

登录到开标系统，找到要参与的项目-“进入网上开标厅”-“点击提交 HASH 编码”-粘贴-立即提交。

说明：①生成的哈希值被保存至区块链上，任何人无法篡改。

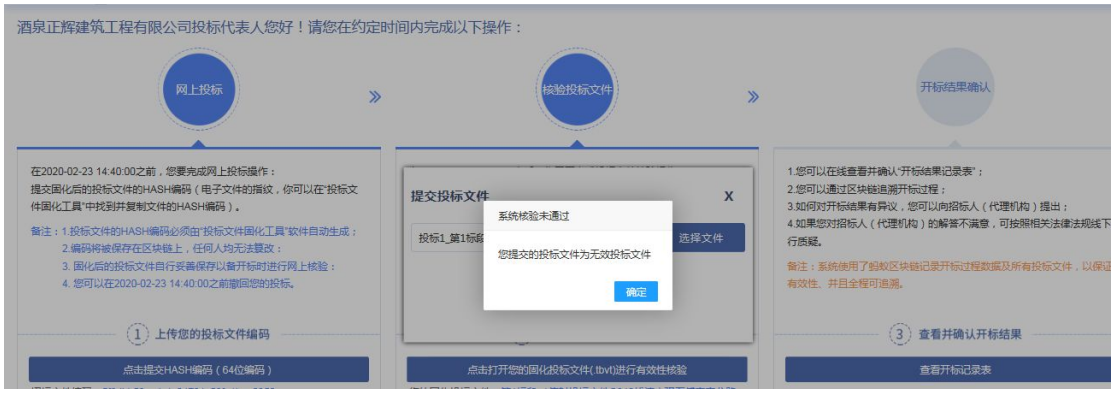
②在开标前可撤回投标重新上传哈希值，以开标前最后一次上传的哈希值为准。

投标人哈希值上传成功，等待开标。

6. 上传电子投标文件

开标之后，投标人登录到开标系统上传电子投标文件。

以上情况代表所上传的电子投标文件与开标前上传的哈希值为一一对应关系，电子投标文件上传成功。



上传电子投标文件时，出现上图情况，代表所上传的电子投标文件与开标前提交的哈希值不对应，请重新选择上传与哈希值对应的电

子投标文件，否则将导致投标失败。

说明：哈希值需要在开标之前提交到开评标系统，并且当前生成的电子投标文件对应唯一一个哈希值，在此期间电子投标文件但凡更改过任何信息，生成之后的哈希值都会发生变化。

7. 确认开标结果

如果对本次开标结果无异议，需确认开标结果。


开标一览表
甘肃省公安厅购置视频会商设备和软终端授权文件项目
序号 投标人 货物名称 数量 单价 总价(万元) 是否递交保证金 是否确认开标结果 区块链查验
1 酒泉正辉建筑工程有限公司 计算机 20 2000 4 已递交 未确认 -
2 天水金思路工程咨询有限公司 1 1 1 1 已递交 未确认 -
3 北京市宾克工程咨询股份有限公司 1 1 1 1 已递交 支付宝扫描二维
可使用钉钉或支付宝扫描查看区块链上本次开标信息。
单击此处
网上投标
核验投标文件
开标结果确认
在2020-02-18 17:05:00之前，您要完成网上投标操作：
提交固化后的投标文件的HASH编码（电子文件的指纹，你可以在"投标文件固化工具"中找到并复制文件的HASH编码）。
备注：1.投标文件的HASH编码必须由"投标文件固化工具"软件自动生成；
2.编码将被保存在区块链上，任何人均无法篡改；
3. 固化后的投标文件自行妥善保存以备开标时进行网上核验；
4. 您可以在2020-02-18 17:05:00之前撤回您的投标。
1 上传您的投标文件编码
点击提交HASH编码（32位编码）
提交的投标文件编码：cb2f4e1b432735709450da4a98266986
提交编码时间：2020-02-18 16:41:04
撤回投标（请慎重操作）
在2020-02-18 17:05:00之后，您需要完成投标文件核验操作：
1.请于在本系统打开您固化投标文件（扩展名为.tbvt)进行有效性核验；
2.如果系统检测到此文件无效，您可以继续寻找并打开正确的固化投标文件；
备注：固化投标文件（扩展名为.tbvt)必须由"投标文件固化工具"软件自动生成，不要进行任何人为修改操作，否则会导致其HASH编码（电子文件的指纹）变化，将肯定无法通过系统核验，因此导致的投标失败后果由投标人自行承担！
2 打开并核验投标文件
点击打开您的固化投标文件(.tbvt)进行有效性核验
您的固化投标文件：投标企业3_第1标段投标文件.tbvt
此文件的HASH编码：cb2f4e1b432735709450da4a98266986
此文件提交完成时间：2020-02-18 17:22:00
1.您可以在线查看并确认"开标结果记录表"；
2.您可以通过区块链追溯开标过程；
3.如何对开标结果有异议，您可以向招标人（代理机构）提出；
4.如果您对招标人（代理机构）的解答不满意，可按照相关法律法规线下进行质疑。
备注：系统使用了蚂蚁区块链记录开标过程数据及所有投标文件，以保证其有效性、并且全程可追溯。
3 查看并确认开标结果
查看开标记录表
开标结果已保存到蚂蚁区块链，任何人均无法进行篡改！你可以使用您的支付宝扫码左侧的二维码查证您的开标结果。
确认对开标结果无异议

本次开标结束。

附件 2

投标文件固化工具用户手册

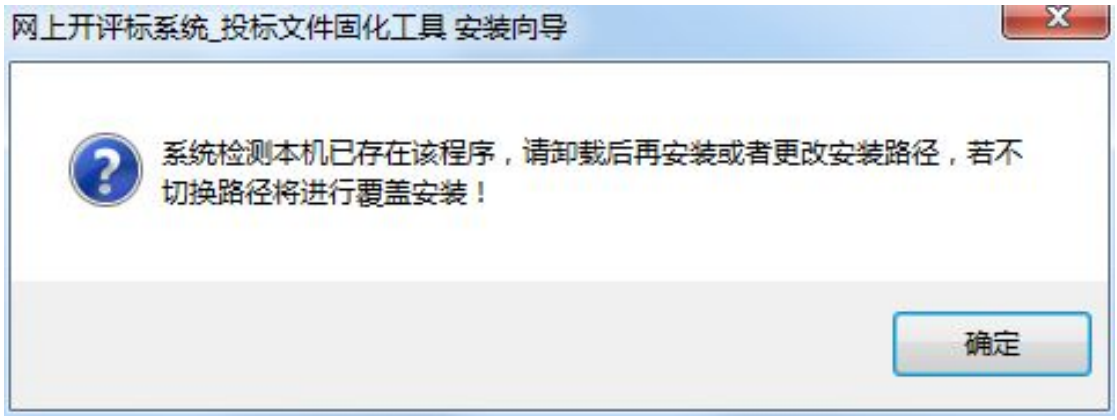
1.系统安装

提示：如果您的电脑安装了 360 安全卫士之类的软件，在下载和安装过程中请先关闭这些软件，否则在下载或安装过程中可能会被误判拦截，导致下载和安装失败。

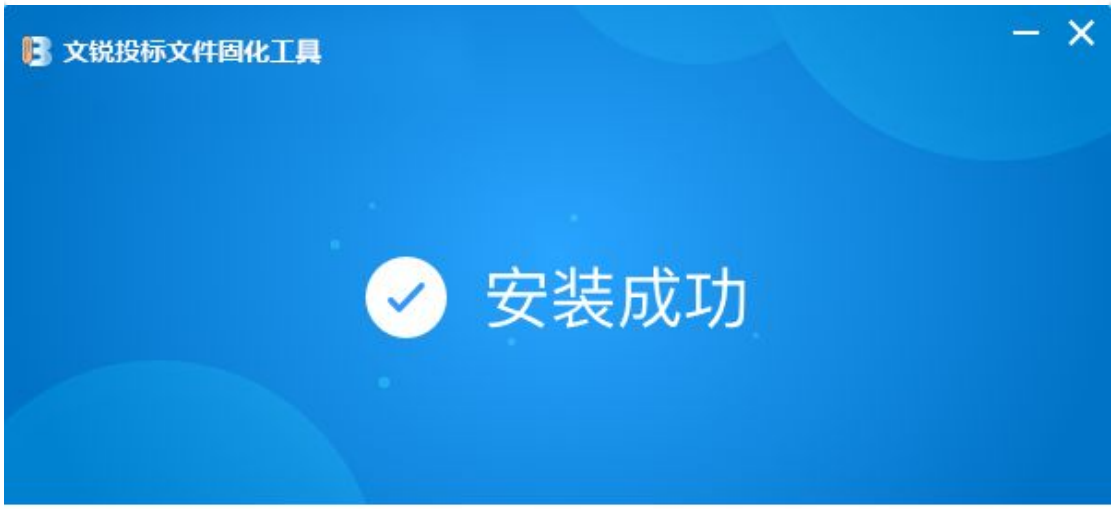
操作系统建议采用 windows7 以上版本。

在线下载软件安装包（点击这里下载）。

打开安装程序（网上开评标系统_投标文件固化工具），如果您没有关闭 360 安全卫士等软件，请在提示窗口中选择“允许程序运行”。如下图所示：


网上开评标系统_投标文件固化工具 安装向导
系统检测本机已存在该程序，请卸载后再安装或者更改安装路径，若不切换路径将进行覆盖安装！
确定


投标文件固化工具
立即安装
《投标文件编制工具用户使用协议》
自定义安装



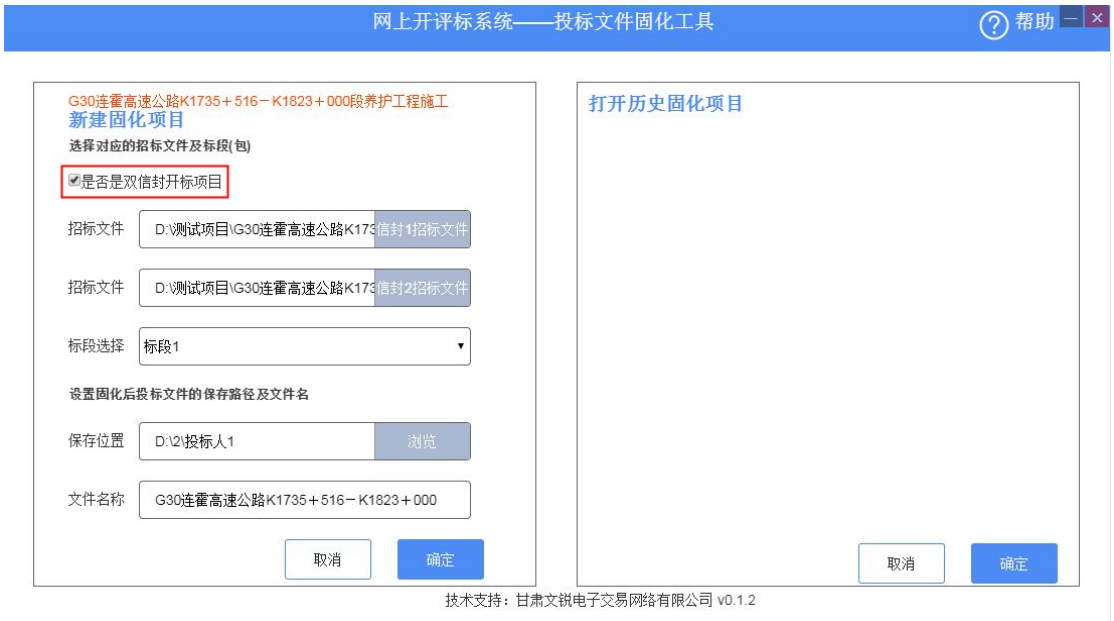
2.使用说明

系统为投标人提供投标文件的设置和固化服务。

在您的电脑桌面上双击 

打开系统，显示如下图所示界面。选择导入您在“网上开评标系统”中下载的“固化后招标文件”，并设置“您的投标文件保存位置”，当前项目的标段数量，然后点击“确定”按钮开始工作。

您也可以在右侧“打开历史固化项目”栏选择并打开以前做过的历史项目。

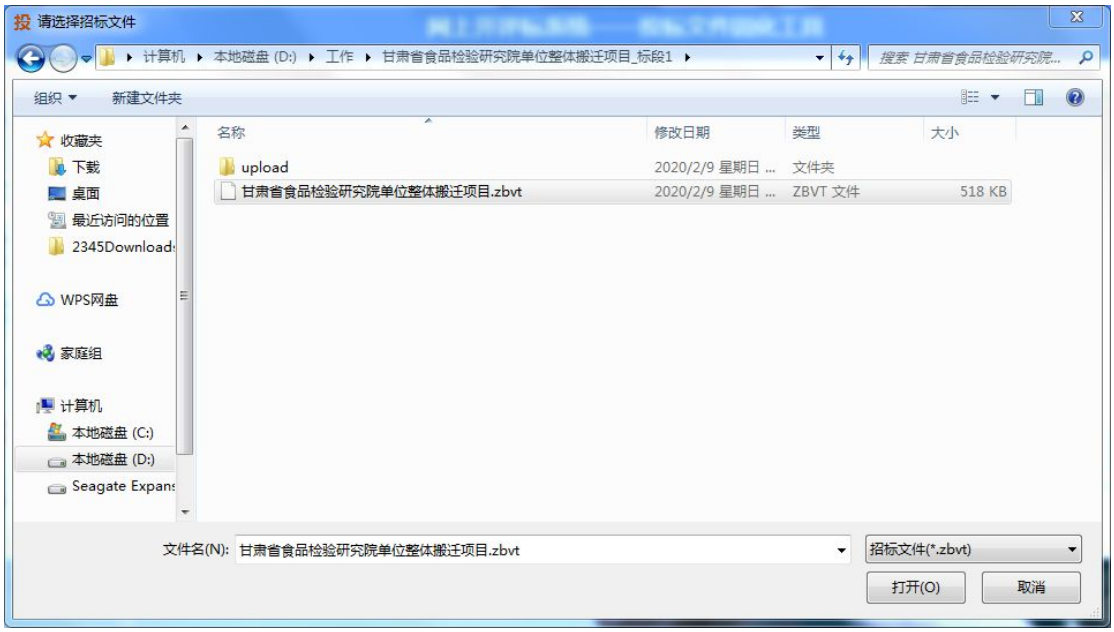


如果您有一个新项目要在线开评标，您要新建一个投标文件固化项目，先选择这个项目的“固化后的招标文件”（注意：是扩展名为 zbvt 的文件，要在网上开评标系统中下载。不是在公共资源交易网上下载的 PDF 版式文件）。

如果项目采用双信封开标方式，您要选中

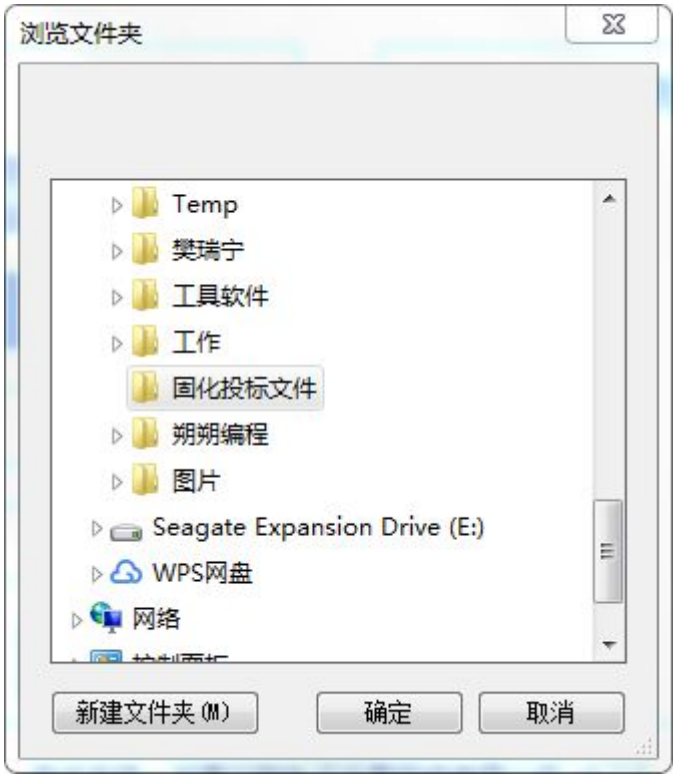
，系统将容许您同时导入两个信封的固化招标文件。

点击“选择招标文件”按钮，打开文件选择窗口选中您下载的这个项目的“固化后的招标文件”，如下图所示：



选择完成后，您要选择当前投标文件对应的标段。

再设置固化后投标文件的保存路径及文件名，方便您找到自己的投标文件。



完成上述设置以后，点击“确定”按钮，打开系统主界面，如下图所示：

例①

例②

完成投标文件的固化，需要完成 4 部分工作：导入投标文件、填写网上开标信息、导入保证金缴款凭证或电子保函、导入法人授权书及授权代表人信息。（**注意：系统所需的所有信息必须填写完整！**）

导入投标文件：

点击“请导入你编制好的投标文件”，选择您编制好的投标文件（PDF 文件），系统自动打开文件，您可以在系统中预览。如果上传有误，您可以重新上传。（注意：必须导入您的投标文件！）

填写开标一览表：

如下图所示，您要按照“固化后的招标文件”的要求填写开标一览表内容并上传对应的开标一览表电子版(表格格式与招标文件有关，内容不一定如下图所示）。（**注意：所有表格必须填写完整，不能漏填任一项！为保证投标报价的一致性，投标人在填写完成开标一览表后，应将填写完成的开标一览表原版打印，然后按要求在打印的开标一览表上签字、盖章，并上传签字、盖章的开标一览表。**）

如果当前项目采用双信封开标方式，您需要分别填写每个信封的开标信息，并上传对应的开标一览表电子版，**请注意报价或日期的单位（元、万元、日历天、工作日、月、年等），不要填错了**。如下图所示：

导入保证金缴款凭证或电子保函：

您需要导入您的投标保证金电汇凭证或电子保函或纸质保函的扫描件，用于开标时帮助工作人员核对保证金到账信息。（**注意：必须导入此项内容！**）

导入法人授权书及授权代表人信息：

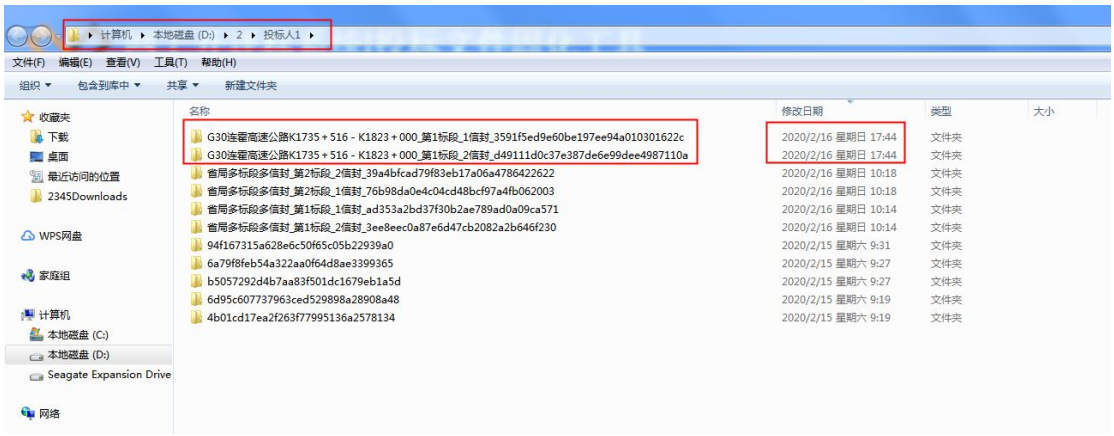
您需要导入您的投标文件中的法人授权书、代理人身份证（正反面）及授权代理人信息，点击“保存身份信息”按钮保存。

如下图所示。（注意：所有内容必须导入和填写完整，不能漏填任一项！）

完成上述 4 项操作后，点击“导出固化文件”按钮。注意：固化后的投标文件（扩展名为.tbvt）必须由当前“投标文件固化工具”软件自动生成，不要进行任何人为修改操作，否则会导致其 HASH 编码（电子文件的指纹）变化，将肯定无法通过系统核验，因此导致的投标失败后果由投标人自行承担！固化投标文件及其对应的 HASH 值已经保存到您设置的工作目录，投标时请准确选择，防止投标失败！

单击确定按钮，系统会自动打开你的工作目录，显示固化后的投标文件及对应的哈希值（HASH 编码），您在“网上开评标系统”中在线投标时要打开 txt 文件拷贝并提交哈希值（HASH 编码）；核验投标

文件有效性时，要使用“固化后的投标文件（.tbvt 文件）”。如下图所示：



完成了投标文件的固化后，您就可在在线进行投标和开标工作了。（具体参见《网上开评标系统用户手册》）

附件 3

“甘肃省公共资源交易局网上开标系统”
投标供应商操作技术支持联系方式

1.技术支持客服电话：0931-4267890

2.技术支持工程师联系方式

姓名	手机号码	钉钉号	QQ 号
韦景霞	18693151517	同手机号码	648715640
宋承艳	19809311390	同手机号码	984837581
寇筱怡	18779298860	同手机号码	980345470