省委编办网络安全等项目

项目编号：ZZCG2020D-GK-107

**公**

**开**

**招**

**标**

**文**

**件**

采购单位：浙 江 省 政 府 采 购 中 心

地 址：杭州市环城北路305号耀江发展中心

**目录**

[**第一章公开招标采购公告 3**](#_Toc496796635)

[**第二章投标人须知 5**](#_Toc496796636)

[**第三章评标办法及评分标准 23**](#_Toc496796637)

[**第四章招标需求 29**](#_Toc496796638)

[**第五章浙江省政府采购合同主要条款指引 24**](#_Toc496796639)

[**第六章投标文件格式附件 96**](#_Toc496796640)

**第一章 公开招标采购公告**

根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《政府采购货物和服务招标投标管理办法》等规定，现就下列项目进行公开招标采购，欢迎提供本国货物、服务的单位或个人前来投标：

一、**项目编号：****ZZCG2020D-GK-107**

**二、公告期限：5个工作日**

**三、采购项目内容、数量及预算**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 标项序号 | 标项名称 | 数量 | 单位 | 预算金额(万元) |
| 1 | 实名制升级改造项目 | 不限 | 项 | 194 |
| 2 | 网络信息安全设施升级改造建设项目 | 不限 | 项 | 310 |
| 3 | 政务云安全服务项目 | 不限 | 项 | 78 |
| 4 | 监理服务项目 | 不限 | 项 | 18 |

**四、合格投标人的资格要求**

符合《中华人民共和国政府采购法》第二十二条和浙财采监【2013】24号《关于规范政府采购供应商资格设定及资格审查的通知》第六条规定,且未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

**投标人的特定条件：**

**标项1、标项2、标项3、标项4:不允许联合体投标**

**五、获取采购文件：**

1 2020年5月8日至20202年5月28日。

2.获取方式：本项目招标文件实行网上获取。供应商登录浙江政府采购网（http://zfcg.czt.zj.gov.cn/）进入政采云系统“项目采购”模块“获取采购文件”菜单，进行网上获取招标文件。

3.招标文件免费获取。

**六、投标保证金：**

投标保证金（人民币）： （空或0元为无需交纳）;

**七、投标截止时间和地点：**

投标人应于2020年5月28日下午17:00时前通过邮寄方式将投标文件密封送交到指定地点，逾期送达或未密封将予以拒收。（授权代表应当是投标人的在职正式职工）。

投标文件收件人：杜鹃鸣，联系方式：0571-88901837，收件地址：杭州市环城北路305号耀江发展中心301会议室。（疫情期间仅接收邮寄方式递交的投标文件,因本大楼疫情管控，推荐使用中国邮政速递和顺丰快递）

**八、开标时间及地点：**

本次招标将于2020年6月1日上午09:00时整在杭州市环城北路305号耀江发展中心二楼开标室开标。

九、本项目采用非现场投递投标文件方式进行投标，供应商询标相关事宜做如下规定：

1. 评标委员会认为需要供应商作出必要澄清或说明，将联系供应商投标文件中的授权代表询标，若无法联系或拒绝澄清说明或澄清说明的内容改变了投标文件的实质性内容的，评标委员会有权对该投标文件作出不利于投标人的评判。

2.供应商应提供电子邮件或传真，评标委员会将通过电子邮件或传真方式将包含询标内容的询标记录表发送至供应商提供的电子邮件或传真。

3. 供应商须将必要澄清或说明填写在询标记录表中，填写完成按招标文件要求签字或盖章后以传真、拍照或扫描后以电子邮件方式递交。

4.本项目开评标过程中询标记录传真号码：0571-88907720；电子邮件地址：563093959@qq.com。本传真、电子邮件仅接受评标委员会要求供应商作出的必要澄清或说明，不接受其他事项。

**十、业务咨询**

|  |  |
| --- | --- |
| **机 构** | 浙江省政府采购中心 |
| **地 址** | 浙江省杭州市下城区环城北路305号耀江发展中心 |
| **网 站** | 浙江政府采购网http://zfcg.czt.zj.gov.cn/（文件下载、公告查询） |
| **咨询事项** | **联系人** | **联系方式** | **传真** | **备注** |
| 项目联系人（A岗） | 杜鹃鸣 | 0571-88901837 | 0571-88907783 | 三楼专业项目采购部]） |
| 项目协办人（B岗） | 吴云飞 | 0571-88907797 | 0571-88907783 |
| 部门负责人 | 高媛沁 | 0571-88907717 | 0571-88907783 |
| 项目保证金 | 邵 幸 | 0571-88907705 | 0571-88907704 | 一楼（服务大厅） |
| 项目监督 | 胡晓霞 | 0571-88907768 | 0571-88907751 | 三楼（采购监督部） |
| 网站系统问题 | 客 服 | 4008817190 | / | 注册、账号、系统操作等 |

**十一、采购需求咨询**

标项1、标项2、标项3：

|  |  |
| --- | --- |
| **采购单位** | 中共浙江省委机构编制委员会办公室（本级） |
| **地 址** | 省府路8号 |
| **咨询事项** | **联系人** | **联系方式** | **传真** | **备注** |
| 采购需求等 | 徐盛彪 | 0571-87057005 |  |  |

**第二章 投标人须知**

前附表

|  |  |  |
| --- | --- | --- |
| 序号 | 内 容 |  要 求 |
| 1 | 项目名称及数量 | 详见《公开招标采购公告》三 |
| 2 | 信用记录 | 根据财库[2016]125号文件，通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn），以开标当日网页查询记录为准。对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的供应商，**其投标将作无效标处理**。 |
| 3 | 政府采购节能环保产品 | 投标产品若属于节能（环保）产品的，请提供参与实施政府采购节能（环境标志）产品认证机构出具的认证证书或证书发布平台的投标产品认证证书查询截图；参与实施政府采购节能（环境标志）产品认证机构详见《市场监督总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告》（2019第16号）；证书发布平台详见《财政部 发展改革委 生态环境部 市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）。产品属于政府强制采购节能品目的（详见《关于印发节能产品政府采购品目清单的通知》财库〔2019〕19号），投标人须按上款要求提供节能产品认证证书或规定网站证书查询截图。**产品属于政府强制采购节能产品品目的，投标人未提供节能产品的，其投标将作无效标处理；本文件“第四章招标需求”另有规定的除外。** |
| 4 | 小微企业有关政策 | 1.根据财库〔2011〕181号的相关规定，在评审时对小型和微型企业的投标报价给予6.0%的扣除，取扣除后的价格作为最终投标报价（此最终投标报价仅作为价格分计算）。属于小型和微型企业的，投标文件中投标人必须提供《小微企业声明函》，并在报价明细表中说明制造商情况。联合体投标时，联合体各方均为小型、微型企业的，联合体视同为小型、微型企业享受政策;联合体其中一方为小型、微型企业的，联合协议中约定小型、微型企业的协议合同金额占到联合体协议合同总额30%以上的，给予联合体 (2-3%)的价格扣除，须同时提供联合体协议约定（包含小型、微型企业的协议合同份额）。2.根据财库[2017]141号的相关规定，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除政策。属于享受政府采购支持政策的残疾人福利性单位，应满足财库[2017]141号文件第一条的规定，并在投标文件中提供残疾人福利性单位声明函（见附件）。3.根据财库[2014]68号的相关规定，在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除政策，并在投标文件中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（格式自拟）。”**(注：未提供以上材料的，均不给予价格扣除）。** |
| 5 | 答疑与澄清 | 投标人如对招标文件有异议，应当于公告发布之日起至公告期限满第7个工作日内，以书面形式向招标采购单位一次性提出，逾期不予受理。 |
| 6 | 是否允许采购进口产品： | 不允许进口产品具体要求详见第四章招标需求各标项的对应内容。 |
| 7 | 是否允许转包与分包 | 转包：否分包：不允许分包 |
| 8 | 是否接受联合体投标 | 标项1:不允许联合体投标;标项2:不允许联合体投标;标项3:不允许联合体投标;标项4:不允许联合体投标接受联合体投标的请提供联合体协议书。 |
| 9 | 是否现场踏勘 | 不组织现场踏勘具体要求详见第四章招标需求各标项的对应内容。 |
| 10 | 是否提供演示 | 不进行演示系统演示具体要求详见第四章招标需求各标项的对应内容。 |
| 11 | 是否提供样品 | 不要求提供样品具体要求详见第四章招标需求各标项的对应内容。 |
| 12 | 投标文件组成 | 投标文件由资质文件、技术及商务文件、报价文件正本**各 1 份**；副本**各****6份**。 |
| 13 | 中标结果公告 | 中标供应商确定之日起2个工作日内，将在浙江省政府采购网(http://zfcg.czt.zj.gov.cn/)发布中标公告，公告期限为1个工作日，服务台根据预留地址寄送中标通知书。 |
| 14 | 投标保证金 | 交纳：投标保证金应按《招标采购公告》六规定交纳。若一次投多个标项，只需交纳一个标项的投标保证金（按所需保证金最大额的标准交纳为准）。退还：中标通知书发出之日起5个工作日内，未中标的投标人提供交入投标保证金时取得的第二联“供应商退款凭据”到招标方服务台办理，招标方以电汇或转账等方式退还投标保证金。 |
| 15 | 合同签订时间 | 中标通知书发出后30日内。 |
| 16 | 履约保证金 | 合同签订时，采购人按《中华人民共和国政府采购法实施条例》有关规定自行收取项目履约保证金。采购人要求中标或者成交供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。履约保证金的数额不得超过政府采购合同金额的10%。 |
| 17 | 付款方式 | 国库集中支付（采购人自行支付）详见各标项的商务要求表 |
| 18 | 投标文件有效期 | 90天 |
| 19 | 投标文件的接收 | 招标方于投标截止时间前五个工作日内接收投标文件，政府采购活动现场确认声明书（格式详见附件）应单独提供。投标人递交投标文件时，如出现下列情况之一的，投标文件将被拒收：1、未按规定密封或标记的投标文件；2、由于包装不妥，在送交途中严重破损或失散的投标文件；3、仅以非纸制文本形式的投标文件；4、未成功办理投标人招标文件获取手续的；5、超过投标截止时间送达的投标文件。投标人在投标截止时间前，可以书面通知（加盖公章）招标方，对所递交的投标文件进行补充、修改或者撤回，补充、修改或者撤回的材料也均通过邮寄方式。补充、修改的内容应当按照招标文件要求签署、盖章、密封后，作为投标文件的组成部分。 |
| 20 | 招标方代理费用 | 0元 |
| 21 | 解释权 | 本招标文件的解释权属于浙江省政府采购中心。 |

**一、总 则**

**（一）适用范围**

仅适用于本次招标文件中采购项目的招标、投标、评标、定标、验收、合同履约、付款等行为（法律、法规另有规定的，从其规定）。

**（二）定义**

1.招标方：指组织本项目采购的浙江省政府采购中心。

2.投标人：指响应招标、参加投标竞争的法人、其他组织或者自然人。

3.采购人：指委托招标方采购本次货物、服务项目的国家机关、事业单位和团体组织。

4.货物：指招标文件规定投标人须向采购人提供的一切材料、设备、机械、仪器仪表、工具及其它有关技术资料和文字材料。

5.服务：指招标文件规定投标人须承担的劳务以及其他类似的义务。

6.项目：指投标人按招标文件规定向采购人提供的需求总称。

**（三）投标人及委托有关说明**

1.授权代表须携带有效身份证件。如授权代表不是法定代表人，须有法定代表人出具的授权委托书（投标文件正本用原件，副本用复印件，格式见附件）。

2.投标人投标所使用的资格、信誉、荣誉、业绩与企业认证必须为本法人所拥有。投标人投标所使用的采购项目实施人员必须为投标人员工（或投标人控股公司正式员工）。

3.以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。

4.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。

5.投标人应仔细阅读招标文件的所有内容，按照招标文件的要求提交投标文件，并对所提供的全部资料的真实性承担法律责任。

**（四）投标费用**

不论投标结果如何，投标人均应自行承担所有与投标有关的全部费用（招标文件有其他相反规定除外）。

**（五）质疑**

1.投标人认为采购文件、招标过程或中标结果使自己的合法权益受到损害的，可以在中标结果公告期限届满之日起7个工作日内，以书面形式一次性向招标方提出质疑。

2.质疑应当以书面形式提出，格式见《政府采购质疑和投诉办法》（财政部令第94号）附件范本，下载网址：浙江政府采购网(http://zfcg.czt.zj.gov.cn/)，位置：“首页-下载专区-质疑投诉模板”。供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

a供应商的姓名或者名称、地址、邮编、联系人及联系电话；

b质疑项目的名称、编号；

c具体、明确的质疑事项和与质疑事项相关的请求；

d事实依据；

e必要的法律依据；

f提出质疑的日期。

供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。质疑应明确阐述招标过程或中标结果中使自己合法权益受到损害的实质性内容，提供相关事实、依据和证据及其来源或线索，便于有关单位调查、答复和处理, 质疑函不符合《政府采购质疑和投诉办法》相关规定的，应在规定期限内补齐的，招标方自收到补齐材料之日起受理；逾期未补齐的，按自动撤回质疑处理。

**（六）招标文件的澄清与修改**

1.投标人应认真阅读本招标文件，发现其中有误或有不合理要求的，投标人应当于公告发布之日起至公告期限满第7个工作日内以书面形式一次性向招标方提出。招标方将在规定的时间内，在财政部门指定的政府采购信息发布媒体上发布更正公告，并以书面形式通知所有招标文件收受人。逾期提出招标方将不予受理。

2.招标方主动进行的澄清、修改：招标方无论出于何种原因，均可主动对招标文件中的相关事项，用补充文件等方式进行澄清和修改。

3.招标文件澄清、答复、修改、补充的内容为招标文件的组成部分。当招标文件与招标文件的答复、澄清、修改、补充通知就同一内容的表述不一致时，以最后发出的书面文件为准。

**二、投标文件的编制**

**（一）投标文件的组成**

投标文件由资质文件、技术及商务文件、投标报价文件三部分组成。

**1.**资质文件

（1）投标声明书 (格式见附件，含重大违法记录声明)；

（2）法定代表人授权委托书(格式见附件)；

（3）提供有效的营业执照复印件并加盖公司公章；事业单位的，则提供有效的《事业单位法人证书》副本复印件并加盖单位公章；自然人的，则提供有效的身份证复印件并签字；

（4）提供有效的依法缴纳税收证明（完税凭证或税务部门出具的证明）；

（5）提供有效的依法缴纳社会保障资金证明（缴纳凭证或人社部门出具的证明）；

（6）联合投标协议书（若需要）;

（7）联合投标授权委托书（若需要）;

（8）提供采购公告中符合投标人特定条件要求的有效的其他资质复印件并加盖公司公章及需要说明的资料。

**2.技术及商务文件**

（1）评分对应表（格式见附件，主要用于评委对应评分内容）

（2）投标项目明细清单（含货物、服务等）；

（3）技术响应表（格式见附件）；

（4）项目总体解决方案（可包含且不限于对项目总体要求的理解、项目总体架构及技术解决方案等）；

（5）项目实施计划（可包含且不限于保证工期的施工组织方案及人力资源安排、项目组人员清单等）；

（6）列入政府采购节能环保清单的证明资料（若有）；

（7）商务响应表（格式见附件）；

（8）售后服务计划（可包含且不限于对用户故障的响应、处理、定期巡检、备品备件、常用耗材提供、驻点人员情况等）；

（9）技术培训计划（若有）；

（10）投标人履约能力（可包含且不限于技术力量情况、投标人各项能力证书）；

（11）案例的业绩证明（投标人业绩情况一览表、合同复印件等）；

（12）投标方认为需要的其他文件资料。

**3.报价文件：**

（1）投标报价明细表（格式见附件）；

（2）投标人针对报价需要说明的其他文件和说明（格式自拟）；

（3）小微企业声明函、网页证明资料（若有，格式见附件）；

（4）残疾人福利企业声明函（若有，格式见附件）。

**注：法定代表人授权委托书、投标声明书、投标报价明细表必须按招标文件格式要求正确签署并加盖投标人公章。资质文件、技术及商务文件中不得出现项目报价信息，否则将作无效标处理。**

**（二）投标文件的语言及计量**

1.投标文件以及投标人与招标方就有关投标事宜的所有来往函电，均应以中文简体字书写。除签名、盖章、专用名称等特殊情形外，投标文件中以中文汉语以外的文字表述部分视同未提供。

2.投标计量单位，招标文件已有明确规定的，使用招标文件规定的计量单位；招标文件没有规定的，应采用中华人民共和国法定计量单位（货币单位：人民币元），**否则将作无效标处理**。

**（三）投标文件的有效期**

1.自投标截止日起90天内投标文件应保持有效。**有效期不足的投标文件将作无效标处理。**

2.中标人的投标文件自开标之日起至合同履行完毕止均应保持有效。

**（四）投标文件的签署和份数、包装**

1.投标人应按本招标文件规定的格式和顺序编制、装订投标文件并标注页码，投标文件内容不完整、编排混乱或装订易脱落导致投标文件被误读、漏读或者查找不到相关内容的，是投标人的责任。

2.投标人应按资质文件、技术及商务文件、报价文件正本、副本规定的份数分别编制并按A4纸规格分别竖面单独装订成册，投标文件的封面应注明“正本”“副本”字样。

3.投标文件的正本需打印或用不褪色的墨水填写，投标文件正本除《投标人须知》中规定的可提供复印件外均须提供原件。副本为正本的复印件。招标方提倡双面打印或书写。

4.投标文件须由投标人在规定位置盖章并由法定代表人或法定代表人的授权委托人签署，投标人应写全称。

5.投标文件不得涂改，若有修改错漏处，须加盖供应商公章或者法定代表人或授权委托人签名或盖章。投标文件因字迹潦草或表达不清所引起的后果由投标人负责。

6.投标人应按资质文件、技术及商务文件、投标报价文件分类分别单独密封封装。投标文件封装后，外包装封面上应注明投标人名称、投标人地址、投标文件名称（资质文件、技术及商务文件、报价文件）、投标项目名称、项目编号、标项及“开标时启封”字样，并加盖投标人公章。

**（五）投标报价**

1.投标文件只允许有一个报价，投标报价应按招标文件中相关附表格式填报，该投标报价应与明细报价汇总相等，且**不允许出现报价优惠等字样（明细出现“0”元，视同赠送）**。

2.投标报价**应包含项目所需全部货物、服务，不得缺漏**，是履行合同的最终价格（含货款、标准附件、备品备件、专用工具、包装、运输、装卸、保险、税金、货到就位以及安装、调试、培训、保修等一切税金和费用）。

3.投标报价总价金额到元为止，如投标报价总价出现角、分，将被抹除。

**（六）投标保证金**

1.投标人须按规定提交投标保证金。

2.保证金形式：网银、汇票、电汇、转帐支票。

3.招标方不接受以现金支票、现金及个人转账方式交纳的保证金。

投标保证金若以网银、电汇方式交纳的,请将网银电脑打印凭证、电汇底单复印件写上所投项目名称、编号、投标联系人、联系电话，请在开标前一个工作日前到招标方服务台开收据。

4.招标方在中标通知书发出后五个工作日内退还投标保证金，供应商办理投标保证金退还时需提供收据的第二联“供应商退款凭据”。**详见浙江省政府采购网**http://zfcg.czt.zj.gov.cn/ ，位置：“首页-网上办事指南-其他-省政府采购中心财务程序-财务程序（一）”

保证金不计息。

**5.投标人有下列情形之一的，投标保证金将不予退还：**

（1）投标人在投标截止时间后撤回投标文件的；

（2）投标人在投标过程中弄虚作假，提供虚假材料的；

（3）中标人无正当理由不与采购人签订合同的；

（4）将中标项目转让给他人或者在投标文件中未说明且未经招标采购单位同意，将中标项目分包给他人的；

（5）其他严重扰乱招投标程序的。

**（七）串通投标认定**

有下列情形之一的，视为投标人串通投标，其投标无效：

1.不同投标人的投标文件由同一单位或者个人编制；

2.不同投标人委托同一单位或者个人办理投标事宜；

3.不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

4.不同投标人的投标文件异常一致或者投标报价呈规律性差异；

5.不同投标人的投标文件相互混装；

6.不同投标人的投标保证金从同一单位或者个人的账户转出。

**（八）投标无效的情形**

在评审时，如发现下列情形之一的，投标文件将被视为无效：

1.未按规定交纳投标保证金的；

2.投标方未能提供合格的资格文件、投标有效期不足的；

3.投标人被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的；

4.投标文件未按招标文件要求签署、盖章的；

5.与招标文件有重大偏离、未满足带“▲”号实质性指标的投标文件；

6.招标需求中要求提供的产品属于节能清单中政府强制采购节能产品品目的，投标人未提供该清单内产品的；

7.资质文件、技术及商务文件中出现投标价格信息的、投标报价超出招标文件中规定的预算金额或者最高限价的；

8.标项以赠送方式投标的、对一个标项提供两个投标方案或两个报价的；

9.评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约，且不能证明其报价合理性的；

10.投标人不接受报价文件中修正后的报价的；

11.未按本章“二、投标文件的编制”第五点投标报价要求报价的；

12.投标文件含有采购人不能接受的附加条件的；

13.投标人被视为串通投标的；

14.不符合法律、法规和本招标文件规定的其他实质性要求的。

**（九）错误修正**

投标文件报价出现前后不一致的，除招标文件另有规定外，按照下列规定修正：

（一）投标文件中报价明细表内容与投标文件中相应内容不一致的，以报价明细表为准；

（二）大写金额和小写金额不一致的，以大写金额为准；

（三）单价金额小数点或者百分比有明显错位的，以报价明细表的总价为准，并修改单价；

（四）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照经投标人加盖公章，或者由法定代表人或其授权的代表签字确认后产生约束力，投标人不确认的，其投标无效。

**三、开、评标程序及评标委员会的评审程序**

**（一）开标程序**

**招标方将按照招标文件规定的时间、地点和程序组织开标，无关人员不得进入开标现场。**

**1.开标会由招标方主持，主持人介绍开标现场的人员情况，宣读接收投标文件的投标人名单、开标纪律、应当回避的情形等注意事项。**

**2.对投标人的投标文件进行查验、核实，由采购人监督人员查验投标文件密封情况并签名确认。**

**3.当众拆封、清点投标文件（包括正本、副本）数量，将其中密封的报价文件现场集中封存保管等候拆封，将拆封后的商务和技术文件由现场工作人员护送至指定的评审地点。**

**4.商务和技术评审结束后，主持人宣告商务和技术评审无效投标人名称及理由，有效投标人的商务和技术得分情况，由工作人员在评标结束后寄回无效投标人的报价文件。**

**5.拆封投标人报价文件，宣读《报价明细表》有关内容，同时当场制作并打印开标记录表，由采购人监督人员、唱标人、记录人和中心现场监督员在开标记录表上签字确认，不予确认的应说明理由。唱标结束后，由评审小组对报价的合理性、准确性等进行审查核实。**

**6.评审结束后，主持人公布中标候选供应商名单，及采购人最终确定中标或成交供应商名单的时间和公告方式等。**

**（二）评标程序**

**招标方将按照招标文件规定的时间、地点和程序组织评标，各评审专家及相关人员应参加评审活动并接受核验、签到，无关人员不得进入评审现场。**

**1.按规定统一收缴、保存评标现场相关人员通讯工具。**

**2.介绍评审现场的人员情况，宣布评审工作纪律，告知评审人员应当回避情形；组织推选评标委员会组长。**

**3.宣读提交投标文件的供应商名单，组织评标委员会各位成员签订《政府采购评审人员廉洁自律承诺书》及各疫情防控类承诺书。**

**4.采购人可以在评标前说明项目背景和采购需求，说明内容不得含有歧视性、倾向性意见，不得超出招标文件所述范围。说明应当提交书面材料，并随采购文件一并存档。**

**5.根据需要简要介绍招标文件（含补充文件）制定及质疑答复情况、按书面陈述项目基本情况及评审工作需注意事项等，让评审专家尽快知悉和了解所评审项目的采购需求、评审依据、评审标准、工作程序等；提醒评标委员会对客观评审项目应统一评审依据和评审标准，对主观评审项目应确定大致的评审要求和评审尺度；对评审人员提出的有关招标文件、投标文件的问题进行必要的说明、解释或讨论。**

**6.采购人代表或由采购人委托的评标委员会对投标人资格文件进行审查并以开标当日为准对投标人“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）信用记录情况进行核实，资格不符合的，应组织相关投标人代表进行陈述、澄清或申辩。**

**7.评标委员会组长组织评审人员独立评审。评标委员会对拟认定为投标文件无效，应组织相关投标人代表通过电话方式进行陈述、澄清或申辩，并以传真或电子邮件方式确认记录；招标方可协助评标委员会组长对打分结果进行校对、核对并汇总统计；对明显畸高、畸低的评分（其总评分偏离平均分30%以上的），评标委员会组长应提醒相关评审人员进行复核或书面说明理由，评审人员拒绝说明的，由现场监督员据实记录；评审人员的评审、修改记录应保留原件，随项目其他资料一并存档。**

**8.做好评审现场相关记录，协助评标委员会组长做好评审报告起草、有关内容电脑文字录入等工作，并要求评标委员会各成员签字确认。**

**9.评审结束后，招标方应对评标委员会各成员的专业水平、职业道德、遵纪守法等情况进行评价；同时按规定向评审专家发放评审费，并交还评审人员及其他现场相关人员的通讯工具。**

**（三）评审程序**

**1.在评审专家中推选评标委员会组长。**

**2.评标委员会组长召集成员认真阅读招标文件以及相关补充、质疑、答复文件、项目书面说明等材料，熟悉采购项目的基本概况，采购项目的质量要求、数量、主要技术标准或服务需求，采购合同主要条款，投标文件无效情形，评审方法、评审依据、评审标准等。**

**3.评审人员对各投标人投标文件的有效性、符合性、完整性和响应程度进行审查，确定是否对招标文件作出实质性响应。**

**4.评审人员按招标文件规定的评审方法和评审标准，依法独立对投标人投标文件进行评估、比较，并给予评价或打分，不受任何单位和个人的干预。**

**5.评审人员对各供应商投标文件非实质性内容有疑议或异议，或者审查发现明显的文字或计算错误等，及时向评标委员会组长提出。经评标委员会商议认为需要供应商作出必要澄清或说明的，以电话方式通知该投标人以书面形式作出澄清或说明。授权代表无法联系或拒绝澄清说明或澄清说明的内容改变了投标文件的实质性内容的，评标委员会有权对该投标文件作出不利于投标人的评判。书面通知及澄清说明文件应作为政府采购项目档案归档留存。**

**6.评审人员需对招标方工作人员唱票或统计的评审结果进行确认，现场监督员应对评审结果签署监督意见。如发现分值汇总计算错误、分项评分超出评分标准范围、客观评分不一致以及存在评分畸高、畸低情形的，应由相关人员当场改正或作出说明；拒不改正又不作说明的，由现场监督员如实记载后存入项目档案资料。**

**7.评标委员会根据评审汇总情况和招标文件规定确定中标候选供应商排序名单。**

**8.起草评审报告，所有评审人员须在评审报告上签字确认。**

**四、评审原则**

**1.评标委员会必须公平、公正、客观，不带任何倾向性和启发性；不得向外界透露任何与评标有关的内容；任何单位和个人不得干扰、影响评标的正常进行；评标委员会及有关工作人员不得私下与投标人接触。**

**2.评审专家因回避、临时缺席或健康原因等特殊情况不能继续参加评审工作的，应按规定更换评审专家,被更换的评审人员之前所作出的评审意见不再予以采纳，由更换后的评审人员重新进行评审。无法及时更换专家的，要立即停止评审工作、封存评审资料，并告知投标人择期重新评审的时间和地点。**

**3.评审人员对有关招标文件、投标文件、样品或现场演示（如有）的说明、解释、要求、标准存在不同意见的，持不同意见的评审人员及其意见或理由应予以完整记录，并在评审过程中按照少数服从多数的原则表决执行。对招标文件本身不明确或存在歧义、矛盾的内容，应作对投标人而非采购人有利的解释；对因招标文件中有关产品技术参数需求表述不清导致投标人实质性响应不一致时，应终止评审，重新组织采购。评审人员拒绝在评审报告中签字又不说明其不同意见或理由的，由现场监督员记录在案后，可视为同意评审结果。**

**4.财政部令第87号《政府采购货物和服务招标投标管理办法》第三十一条规定：使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个投标人获得中标人推荐资格，招标文件未规定的采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。**

**非单一产品采购项目，采购人应当根据采购项目技术构成、产品价格比重等合理确定核心产品，并在招标文件中载明。多家投标人提供的核心产品品牌相同的，按前款规定处理。**

**五、确定中标供应商的原则**

 1.项目由评标委员会根据第三章《评标办法与评分标准》规定提出中标候选人排序。

 2.采购人应当自收到评标报告之日起５个工作日内，在评标报告确定的中标候选人名单中按顺序确定中标人，或者采购人委托评标委员会在评标报告确定的中标候选人名单中按顺序确定中标人。采购人在收到评标报告5个工作日内未按评标报告推荐的中标候选人顺序确定中标人，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标人。

 3.采购结果经采购人确认后，招标方将于2个工作日内在浙江省政府采购网上发布中标公告，并向中标方签发书面《中标通知书》，服务台根据预留地址寄送中标通知书。

**六、合同授予**

**（一）签订合同**

1.采购人与中标人应当在《中标通知书》发出之日起30日内签订政府采购合同，招标方作为合同签订的鉴证方。

2.中标人拖延、拒签合同的,将被扣罚投标保证金并取消中标资格。

**（二）履约保证金**

1.合同签订时，采购人按《中华人民共和国政府采购法实施条例》有关规定自行收取项目履约保证金。采购人要求中标或者成交供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。履约保证金的数额不得超过政府采购合同金额的10%。

2.按合同约定办理履约保证金退还手续。

**七、货款的结算**

货款由采购人按招标文件规定的付款方式自行支付。若资金在采购人处的，由采购人直接支付；若资金在核算中心的，由采购人向核算中心发起支付令，由核算中心把货款打入中标商帐户。

**第三章 评标办法及评分标准**

根据《中华人民共和国政府采购法》等有关法律法规，结合本项目的实际需求，制定本办法。

**一、总则**

本次评标采用综合评分法，总分为100分。合格投标人的评标得分为各项目汇总得分，中标候选资格按评标得分由高到低顺序排列，得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按技术得分由高到低顺序排列。评分过程中采用四舍五入法，并保留小数2位。

**二、分值的计算**

技术、资信、商务及其他分按照评标委员会成员的独立评分结果汇总后的算术平均分计算，计算公式为：

技术、资信商务及其他分=评标委员会所有成员评分合计数/评标委员会组成人员数

投标人评标综合得分=价格分+(技术分+资信商务及其他分)

**三、评标内容及标准**

**标项1的评分方法**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 评分类型 | 评分标准 | 分值 |
| 1 | 报价 | (最低报价/投标报价)\*最大分值 | 10 |
| 1 | 技术 | 功能需求：对项目需求的理解，要求投标方提供需求规格说明书。 | 20 |
| 2 | 技术 | 非功能需求：软件质量的稳健性、安全性、可操作性、可扩充性、可维护性、可移植性等。软件所运行的环境：从功能上来支撑软件运行所需要的条件。 | 14 |
| 3 | 技术 | 功能点及架构：软件整体架构与功能点的可行性、合理性、规范性，与用户现有系统的兼容性，包括总体设计、接口设计、系统数据结构设计、数据库设计及模块设计等。 | 12 |
| 4 | 技术 | 测试方案、进度控制计划 | 7 |
| 5 | 技术 | 软件开发工程量计算(技术文件中提供不含价格的工程量计算清单，要求到人\*天，格式自定) | 5 |
| 6 | 技术 | 项目组人员个人、团队开发能力情况（资历及业绩） | 10 |
| 7 | 商务资信 | 对接及数据迁移方案 | 4 |
| 8 | 商务资信 | 售后服务的响应情况（对用户故障响应、处理等） | 3 |
| 9 | 商务资信 | 项目维护计划（驻点人员安排，定期巡检等情况）的有效性等 | 3 |
| 10 | 商务资信 | 培训方案、计划的可行性及合理性 | 2 |
| 11 | 商务资信 | 公司技术力量情况等 | 5 |
| 12 | 商务资信 | 经验及业绩(类似项目开发成功案例) | 3 |
| 13 | 商务资信 | 投标书编制质量 | 2 |

**标项2的评分方法**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 评分类型 | 评分标准 | 分值 |
| 1 | 报价 | (最低报价/投标报价)\*最大分值 | 30 |
| 1 | 技术 | 符合明确指标参数得22分。对非关键的性能指标及技术参数属负偏离或缺漏项的每项扣3分（若负偏或缺漏项5个以上的按重大偏离处理）。 | 22 |
| 2 | 技术 | 对性能指标、技术参数属正偏或高配的、有先进程度的正偏离每项加1分（最高分为5分），无实质性意义的正偏离不加分。 | 5 |
| 3 | 技术 | 提供市场监管总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告（2019第16号）通过《参与实施政府采购节能产品认证机构名录》认证机构认证的环境标志产品认证证书或者证书的查询网址及截图的，得1分, 节能产品认证证书或者证书的查询网址及截图的，得1分。 | 2 |
| 4 | 技术 | 系统集成的具体技术解决方案。 | 7 |
| 5 | 技术 | 项目系统集成具体实施计划。 | 6 |
| 6 | 技术 | 系统集成项目组实施人员能力。 | 6 |
| 7 | 商务资信 | 项目维护计划（驻点人员安排，定期巡检，备品备件等情况）的有效性等。 | 5 |
| 8 | 商务资信 | 售后服务的响应情况（对用户故障响应、处理等）。 | 5 |
| 9 | 商务资信 | 培训方案、计划的可行性及合理性。 | 2 |
| 10 | 商务资信 | 公司技术力量情况。 | 5 |
| 11 | 商务资信 | 经验及业绩（详见商务要求表）。 | 3 |
| 12 | 商务资信 | 投标文件编制有序、装订整齐、书面整洁、内容详实。 | 2 |

**标项3的评分方法**

|  |  |  |
| --- | --- | --- |
| 评分项目 | 分值 | 评标要点及说明 |
| 投标报价（20分） | 20 | 项目成本构成合理、满足招标文件要求且报价最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：投标报价得分=（评标基准价/投标报价）\*20 |
| 技术（62分）      | 20 | 符合明确需求参数得20分。对非关键的需求指标及技术参数负偏或缺漏项的每项扣3分（若负偏或缺漏项5个以上的，按重大偏离处理）。 |
| 2 | 需求指标属于正偏的、有先进程度的每项加1-2分（最高分为2分）。无实质性意义的正偏离不加分。 |
| 8 | 项目实施方案。 |
| 12 | 项目质量：包括项目质量体系、质量安全与保密控制、质检及验收方案等（详见招标需求）。 |
| 10 | 项目配套设备：包括项目配套软硬件设备等（详见招标需求）。 |
| 10 | 项目组人员个人、团队服务能力情况（资历及业绩）（具体对应招标需求）。 |
| 商务（18分）       | 3 | 项目维护计划（服务人员安排，定期巡检等情况）的有效性等（具体对应商务要求表）。 |
| 3 | 售后服务的响应情况（对用户故障响应、处理等）（具体对应商务要求表）。 |
| 2 | 培训方案、计划的可行性及合理性（具体对应商务要求表）。 |
| 5 | 公司技术力量情况（具体对应商务要求表）。 |
| 3 | 经验及业绩（具体对应商务要求表）。 |
| 2 | 投标文件编制质量。 |

**标项4的评分方法**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 评分类型 | 评分标准 | 分值 |
| 1 | 报价 | (最低报价/投标报价)\*最大分值 | 20 |
| 1 | 技术 | 对项目需求的理解、监理难点、要点分析是否准确全面，关键点的控制等是否符合实际监理服务要求。 | 8 |
| 2 | 技术 | 监理大纲或监理规划是否规范、可行性和完整性4分；监理具体实施方案及细则是否规范、可行性和完整性6分。 | 10 |
| 3 | 技术 | 监理建议的合理性及其监理相应的措施的可行性。 | 6 |
| 4 | 技术 | 质量控制：分阶段质量控制的重点等方法和措施4分；进度控制：分阶段进度控制的目标、任务等方法和措施4分；投资控制：成本核算、变更控制等方法和措施2分。 | 10 |
| 5 | 技术 | 合同管理2分；信息管理：各阶段的文档管理（含技术文档和建设过程文档）4分；信息安全管理2分；组织协调的方法和措施4分。 | 12 |
| 6 | 技术 | 监理项目组人员个人能力情况（数量、职业资格、技能证书、实施经验、社保、从业时间）6分；监理团队能力情况4分；总监理工程师情况（职业资格、技能证书、实施经验、社保、从业时间）4分。 | 14 |
| 7 | 技术 | 监理技术人员到位率和人员稳定性方面的保障措施，驻场人数及人员应急措施。 | 3 |
| 8 | 商务资信 | 监理服务保障措施和后续监理支持情况。 | 5 |
| 10 | 商务资信 | 公司综合实力。（具体详见商务要求表） | 5 |
| 11 | 商务资信 | 项目监理案例及实施经验。（具体详见商务要求表） | 5 |
| 12 | 商务资信 | 编制有序、装订整齐、书面整洁、内容详实。 | 2 |

**第四章招标需求**

**特别说明：**

**1.根据浙财采监字[2007]2号文件规定：除采购文件明确的品牌外，欢迎其他能满足本项目技术需求且性能与所明确品牌相当的产品参加。**

**2.需求中不允许偏离的实质性要求和条件，以“▲”号标明，如投标人未响应的，将被视为无效。**

**3.核心产品在各标项内容中明确，如出现同品牌情况的，评标委员会根据评审原则第4条规定执行。**

**4.采购人拟采购的产品属于政府强制采购节能品目的，（详见《关于印发节能产品政府采购品目清单的通知》财库〔2019〕19号），需按《财政部 发展改革委 生态环境部 市场监管总局 关于调整优化节能产品、环境标志产品政府采购执行机制的通知》财库〔2019〕9号要求执行，但无对应细化分类或节能清单中的产品无法满足工作需要的，采购人应当在详细需求中标明并说明理由，否则按照前附表第三点要求执行。**

**标项1:** **实名制升级改造项目**

一、建设内容

（一）实名制系统升级

**1.根据中央编办要求调整完善系统指标项。**根据2020年中央编办对机构编制实名制管理业务的数据项变更描述，以及中央机构编制实名制系统对字典项的调整，进行本地化实名制系统指标项升级。配合各市做好本地部署的实名制系统接口和指标的升级改造工作，确保全省实名制数据的互联互通，及时完成向中央报送我省实名制月报和机构编制年报的任务。

**2.完善机构编制统计资料汇编功能和历年年报留痕功能。**根据业务需求完善统计资料汇编功能，开发对历年机构编制统计年报留痕功能，方便查询查看。

**3.完善系统内单位数据列表显示功能。**完善系统内单位数据列表显示功能，能够对单位的实有人员指定排序项。单位有查询本单位内设、下设机构和下属事业单位数据的功能。系统管理员可以通过系统管理对实有人员界面要显示的指标项进行自定义编辑。

**4.增加业务限制功能。**在系统中实现超编限制入编、超职数限制加职数等功能，包括单位的职数总数不能超过编制数的限制。

**5.加强实有人员菜单下的查询功能。**加强实有人员菜单下的查询功能，在查询条件后增加更多选项，如“在编状态”“编制类型”“所在处室”“性别”“出生年月”“是否公务员登记”等查询条件项。同时，实有人员菜单中，添加“查询本系统”选项，可查询全系统包括下设、事业单位人员情况。

**6.增加人员信息变动记录。**在人员信息中，增加履历，汇总记录在编人员调动、转任、职务变动等情况。

**7.强化离退休人员管理。**在现有“离退休人员”模块中，只有“删除”、“打印”、“导出”三种功能，需要在现有功能的基础上，增加“修改”和“划转”的功能。

**8.完善通知、公告功能。**编办管理员可以在系统内向本辖区单位指定账户（支持批量）发送通知（可带附件），接收单位的账户在首次登录时自动弹出在系统登录首页面。

**9.开发人社厅和省医保局业务协同功能。**根据机关内部“省属事业单位工作人员交流（调动）”“一件事”联办要求，配合省人社厅和省医保局做好业务协同和系统功能开发。

**10.增加执法队伍汇总查询模块。**完善执法队伍业务指标项，对执法队伍进行精细化管理，并增加数据汇总、分析、统计报表功能。

**11.完善传统台账功能。**实名制系统中原有台账编制数、内设机构个数、领导职数是为了调整计算过程而设计的，难以体现传统台账的直观、便捷、记录内容的多样性等要求。根据业务需求进一步完善系统自动生成传统台账功能。

**12.完善五年内预计退休人员功能。**在实有人员模块中，可选择查看一年内、两年内、三年内、四年内、五年内退休人员情况的基础上，根据男女退休年龄不同进行逻辑判断。并支持退休人员列表的导出功能，以及退休人员详细信息查询功能。

**13.完善查询功能。**在自定义查询中，保留个人历史查询记录，便于下一次查询。对机构情况中，机构设置情况及编制情况的实有数增加反查功能。

**14.完善报表功能。**根据业务需求开发所需的相关报表。

（二）实名制系统重构、界面设计和帮助功能完善

重新设计系统的前端展示平台，强化系统访问的稳定性和兼容性，对系统底层和前端框架进行升级，要求遵循原生 HTML/CSS/JS 的书写与组织形式，具有友好的操作体验，兼容火狐等各类浏览器等，保证页面效果稳定，不变形、不报错，页面实现效果流畅。优化系统帮助功能，通过操作指南、使用和填报说明、动画演示等形式丰富系统帮助功能，提升用户体验。

（三）完善工资统发数据比对功能

升级完善与省级工资统发系统数据网络比对功能。规则及流程如下：

1.比对以单位同一社会信用代码为标准，逐个单位去比对在职人员信息。

2.比对结果中，若人员信息未在实名制系统中，则提示单位用户在实名制系统中对该人员做增编操作，保持与人社系统人员同步。

3.比对结果中，若实名制系统中人员未在统发系统中，则提示单位用户在实名制系统中对该人员做减少操作，保持与统发系统人员同步。

4.比对结果中，若实名制系统中人员领导职务和综合管理类公务员职级和统发系统比对不一致，则提示单位用户在实名制系统中对该人员进行修改，保持与统发系统人员同步。

5.比对结果中，若实名制系统中人员未填写行政职务，而统发系统中已经填写，则提示单位用户在实名制系统中对该人员进行修改，保持与统发系统人员同步。

6.各单位的比对结果将发送到实名制系统对应单位用户，并提醒该单位人员信息的变更；同时所有比对不一致提示给编办用户，督促编办用户尽快处理这些业务。

7.比对基础数据、比对过程数据及比对结果数据的统一管理。

8.对各类人员变动的比对结果进行分析，对问题多发、频发的单位发送通知，对后续工作进行督促。

（四）完善与省养老保险系统数据共享

升级完善与省养老保险系统数据对接、比对、共享功能。规则和流程如下：

1.比对以单位同一社会信用代码为标准，逐个单位去比对在职人员信息。

2.比对结果中，若人员信息未在实名制系统中，则进入实名制人员自动入编的流程中，对该人员做增编操作，保持与养老保险系统人员同步。

3.比对结果中，若实名制系统中人员未在统发系统中，则进入实名制人员自动减编的流程中，对该人员做减少操作，保持与养老保险系统人员同步。

4.各单位的比对结果将发送到实名制系统对应单位用户，并提醒该单位人员信息的变更；同时所有自动入、减编信息提示给编办用户，督促编办用户尽快处理这些业务。

5.比对基础数据、比对过程数据及比对结果数据的统一管理。

6.对各类人员变动的比对结果进行分析，对问题多发、频发的单位发送通知，对后续工作进行督促。

（五）开发数据校验系统

实现对实名制各类表格录入信息进行信息校验，增加一些填报内容的逻辑检验关系，可以在用户填报时进行校验提醒，并设置集中的校验功能模块，对全局数据进行校验。校验结果可通过系统推送，并作为月报年报的报送前置。数据验证包含：

1.机关的机构代码不是15字节长度。

2.行政--树节点名称和详细信息中机构名称不一致。

3.行政机构下存在行政机构。

4.行政机关台账为空。

5.内下设-树节点名称和详细信息中机构名称不一致。

6.下设机构台账为空。

7.事业单位台账为空。

8.街道乡镇--树节点名称和详细信息中机构名称不一致。

9.事业-树节点名称和详细信息中机构名称不一致。

10.事业单位行业分类不在字典项中。

11.事业单位行业分类没选到叶子结点。

12.行政机构存在两种编制类型的人员。

13.事业单位存在两种编制类型的人员。

14.行政机构含有机关其他编制。

15.除群团系统外，其他行政机构存在事业编制。

16.人员选择机关其他编制的。

17.机构编码为空。

18.机构性质和系统类别不对应的情况（党委下只能有政党机关和其他）。

19.机构性质和系统类别不对应的情况（政府下只能有国家机关、政法机构和其他）。

20.下设机构的隶属单位为空。

此外，对照中央编办实名制系统校验项对系统校验进行优化。

（六）整合数据采集分析系统

将此前建设的数据采集分析系统功能集成整合并入到实名制管理系统，进一步提升系统的使用效率，避免因多头建设、使用率不高而导致的浪费，节约经费。整合后，该功能集数据抓取、过滤、明义、梳理、入库于一体，智能数据对接，通过数据建模实现多种复杂的场景式分析功能。主要用于对所辖区域的机构编制总体情况进行全面掌握，随时了解各区划、各类型编制、职数的整体情况和变化趋势。数据分析功能模块以实名制系统数据为基础，以多维度、精细化的数据分析准确掌握机构编制资源配置现状，开展机构编制动态研判分析，确保出台政策合理可行，进而发挥实名制系统信息在控编减编、机构编制管理、深化行政体制改革等工作中的基础支撑作用。

**1.开发基础数据模型。**根据省市编办的统计需求，系统生成基础统计模型，各类模型均支持省、市、县3级区划点击查看。

基础统计模型包括：

（1）各级各类机构编制和实有人员情况（按层级）

（2）各级各类机构编制和实有人员情况（按区划）

（3）厅级以上领导职数情况（按层级）

（4）厅级以上领导职数情况（按区划）

（5）党政群系统机构编制和实有人员情况（按层级）

（6）党政群系统机构编制和实有人员情况（按区划）

（7）政法系统机构编制和实有人员情况（按层级）

（8）政法系统机构编制和实有人员情况（按区划）

**2.定制统计模型。**在原有基础统计模型之上进行定制开发，形成个性化的各类统计图表，辅助各类用户精确掌握机构编制的各种情况。

**3.设置大屏展示功能**

根据编办实际需要，对机构编制总体情况、变化情况、预警情况等进行大屏幕展示，并可定时切换展示场景。

（七）加强数据安全

**1.对密码传输加密。**根据编办需要，采用https进行密码传输，或使用sha256哈希算法进行加密。

**2.完善数据备份机制。**采用稳定可靠的数据实时备份解决方案开展对实名制系统的实时备份。

**3.集成电子公章功能。**在实名制系统的用编审核中集成电子公章功能，实现部门申报和编办审核加盖电子公章。

**4.配合开展对数据传输加密功能**。根据编办需要，配合相关安全公司，对实名制存储和传输的数据进行加密。

**5.完善日志功能。**对系统的增删改查等操作进行有效记录。

（八）制作实名制管理介绍短片。时间控制在5分钟左右，主要是介绍我省实名制管理工作历史背景、主要做法和取得成果。

（九）引入公安照片。开发信息查询接口，通过省公共数据共享平台，引入省公安厅居民身份证照片。

（十）完善编外用工统计模块。根据机关部门和事业单位编外用工管理需求，对现有功能进行升级改造，区分编外聘用人员、人事代理、劳务派遣和其他4种类型，开发独立模块，植入计算方式。

（十一）完善周转编制管理模块。根据周转编制管理需要，进一步完善功能设计，实现对周转编制和实有人员进行锁定管理。

（十二）增加台账修改的留痕日志。对编办用户进行台账修改留痕管理，用户名和修改内容可实时查看。

（十三）开发与事业单位登记系统的数据共享功能。开发信息查询接口，实现与事业单位登记系统信息协同共享。

二、采购清单及数量

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 采 购 内 容 | 单位 | 预算（万元） | 使用单位 |
| 1 | 机构编制实名制管理系统升级项目 | 1套 | 194 | 省委编办 |

三、系统验收要求

中标方在采购人指定场所完成许可软件的安装和调试工作（包括个性化改造及适应性修改部份），并与采购人一起按软件的需求说明书或使用手册规定的技术指标和参数对该软件进行验收测试，验收测试合格后，采购人和中标方代表共同在验收合格证明书上签字。

四、验收方式

项目实施完成后由采购人负责组织验收。

五、项目组人员团队要求

1、项目经理具有全日制计算机专业本科及以上学历，毕业15年以上，具备人力资源和社会保障部门颁发的信息系统项目管理师证书，且具备机构编制类项目管理经验。提供担任机构编制类项目经理的证明材料、具体负责的项目名称及项目联系人、联系方式、学历复印件、人员资质证书复印件。不提供不得分。（4分）

2、数据库工程师具有国家有关部门颁发的数据库系统工程师证书和系统集成项目管理证书，具有机构编制类项目开发经验。提供近三个月社保证明材料复印件、证书复印件、机构编制类项目经验证明材料、具体负责的项目名称及项目联系人、联系方式。不提供不得分。（3分）

3、除项目经理和数据库工程师之外，拟投入的项目组人员不少于20人，组员中有不少于15人具有机构编制类项目开发经验，组员中至少三人具备国家有关部门颁发的软件开发相关证书。提供近三个月社保证明材料复印件、人员名单、角色分工、简历、证书复印件、机构编制类项目经验证明材料、具体负责的项目名称及项目联系人、联系方式。不提供不得分。（2分）
4、提供至少3人的驻场服务，其中驻场开发至少2人，要求驻场人员有机构编制类项目驻场开发和服务经验，具体负责的项目名称及项目联系人、联系方式。（1分）

**商务要求表**

|  |  |
| --- | --- |
| **▲供货时间（项目工期）及地点** | 合同签订之日起6个月内完成项目实施并通过验收。 |
| **▲付款条件（明确是否需要履约保证金）** | 合同签订后20日内，支付合同总价格的50%；通过验收并投入运行后20个工作日内支付合同总额的50%。 |
| **违约责任及争议解决方式** | 如无特别说明，按“浙江省政府采购合同主要条款指引”相关违约责任及争议解决方式内容。 |
| **售****后****服务** | **项目维护计划** | 中标方须向采购人提供良好的技术支持。项目验收完成后要提供一年的免费技术服务。 |
| **响应情况** | 在保证期内，采购人提出服务要求后2小时做出响应，8小时内到达现场。能够提供驻场售后服务，质保期内需提供至少三名驻场售后服务人员,进驻服务前需向采购人提供与驻场售后服务人员签订的劳动合同复印件。 |
| **技术培训** | 中标方需采用集中培训的方式对用户进行软件的应用及相关培训，使用户能够理解并熟练掌握标准业务流程的操作。 |
| **履约能力** | **公司技术力量情况** | 具有高新技术企业证书的得 （1分）具有软件企业证书和软件产品证书的得 （1分）具有质量管理体系认证证书ISO9001的得 （1分）具有机构编制类计算机软件著作权登记证书，每提供一个得1分，未提供不得分，最多得2分（2分） |
| **经验或业绩要求** | 自2017年1月1日以来类似成功项目业绩，提供合同复印件需加盖公章。（每提供一个得一份，最高3分） |

#

# 标项2:网络信息安全设施升级改造建设项目

## 一、项目概述

**（一）项目背景**

省委编办信息化经过近些年建设和发展，已经形成了由电子政务内网（机密网）、电子政务外网、互联网等网络组成的电子政务网络体系，满足了内部人员网上办公、部门之间业务协同、信息网上交互及为社会公众服务的网络环境需求，有效支撑了实名制、事业单位网上登记管理、办公自动化、门户网站等电子政务应用系统的长效运行，基本实现了近些年部门信息化建设的相关需求。但是，随着时间推移，部分信息化硬件设施设备已经开始出现老化且功能、性能较现技术也日趋落后。特别是网络安全设施设备，大部分都是在2011、2012年采购及投入使用，至今不间断运行已超过7年（已接近正常的8年更新期）。为继续确保相关系统正常、稳定运行，一是需为已超出免费质保和运维期的软硬件设备采购产品维保和升级服务；二是需结合新现状、新形势、新要求，开展已老化设备的更新和升级迭代；三是需加强对信息系统数据安全保护，构建数据安全防护系统，提升关键应用和核心数据保护和防控能力。

**（二）项目目标和内容**

1．项目目标

根据等级保护新要求，围绕当前已形成的电子政务网络体系，构建功能齐全、设施完善、运行稳定的网络安全防护平台，确保我办现有各电子政务应用系统安全稳定运行，有效保障部门数字化转型推进，持续提高电子政务、行政效能和计划管理水平。

2．主要建设内容

（1）更新已到使用年限的关键网络安全设施

更新已到使用年限的关键设备（关系网络全局运行和核心数据安全的软硬件设备）；更新功能和性能无法满足要求的设备（包括：日志审计系统等）；根据等级保护相关要求，进一步完善网络安全防护体系（包括：网络防病毒功能等）。

（2）构建数据安全防护系统，提升关键应用和核心数据保护和防控能力

集成数据库加密、数据库安全防护类安全产品，建立完善数据全生命周期的安全保障措施,确保数据采集与预处理、数据存储、数据应用、数据传输和数据销毁过程中的安全。采用有效的技术手段实现数据分类、核心数据加密，保障信息系统中关键业务数据以及个人信息的完整性、保密性和可用性要求。利用主动动态防御技术，实现应用系统和网站页面的一次性加密，有效弥补传统的安全产品不能有效应对攻击方式的变化,有效补充动态防护、主动防御安全能力，从而进一步提升数据安全防控能力。

（3）根据等保2.0要求，强化和完善应用系统安全日志功能

根据《网络安全法》和等级保护2.0相关要求，优化日志留存功能,提升日志审计覆盖范围,加强应用系统日志权限管理。

（4）健全网络安全管理运行体系

根据信息系统安全等级保护要求，一是构建网络管理平台，实现各网络平台、各电子政务应用系统运行实时监控，实现运行情况可视化管理；二是建立安全运行管理规范和制度，实现规范化、标准化运行机制。三是开展重要网站和信息系统常态化安全监测，包括应用层漏洞、挂马、暗链、篡改、敏感字、主机漏洞等进行安全监测，及时发现安全隐患。

## 二、采购内容

### 采购项目

本次项目采购内容包括：网络安全信息设施更新、数据安全防护系统、应用系统的安全服务及整体项目集成工作。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **主要规格描述** | **数量** |
| **一** | **网络安全信息设施更新** |  |
| 1 | 网络防火墙 | 详见采购需求中技术要求。 | 4 |
| 2 | 上网行为管理设备 | 详见采购需求中技术要求。 | 1 |
| 3 | WEB安全防护系统 | 详见采购需求中技术要求。 | 1 |
| 4 | 数据库审计设备 | 详见采购需求中技术要求。 | 1 |
| 5 | 日志审计设备 | 详见采购需求中技术要求。 | 1 |
| 6 | 负载均衡设备 | 详见采购需求中技术要求。 | 1 |
| 7 | 网络防毒墙 | 详见采购需求中技术要求。 | 1 |
| 8 | VPN设备 | 详见采购需求中技术要求。 | 1 |
| 9 | **数据备份一体机 （核心产品）** | 详见采购需求中技术要求。 | 1 |
| 10 | 堡垒主机 | 详见采购需求中技术要求。 | 1 |
| 二 | **数据安全防护系统** |  |
| 1 | 加密服务平台 | 提供数据加解密以及密钥安全管理功能，确保数据加密算法及密钥的安全性，支持国家密码管理局规定的商用密码算法，包括SM2、SM3、SM4算法。产品需拥有商用密码型号资质。详见采购需求中技术要求。 | 1 |
| 2 | 数据库安全防护平台 | 系统提供数据库加密、数据库防火墙、数据库安全访问控制、图形化配置管理、操作日志审计等安全功能。支持集群化部署，防止单点故障。详见采购需求中技术要求 | 1 |
| 3 | WEB应用安全防护平台 | 具有主动防御、动态防御应用安全功能，有效防止防止BOT攻击，非法爬虫，暴力攻击，确保应用层系统的安全平稳运行；支持集群化部署，防止单点故障。详见采购需求中技术要求 | 1 |
| **三** | **应用系统安全服务** |  |
| 1 | 应用系统安全服务 | 应用系统的安全服务主要包括：驻场服务、资产调查、数据备份、运行监控、网络安全防范及评估服务、病毒查杀服务、网站实时监控、等保测评辅助、应急响应等服务。详见采购需求中技术要求 | 1项 |

### 采购指标需求

**1．网络安全信息设施更新技术要求**

**（1）网络防火墙（4台）**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 性能规格 | 最大吞吐量≥10Gbps，并发连接数≥250万，每秒新建连接≥15万/秒，提供三年硬件维修服务. |
| 硬件规格 | 2U机箱，接口≥6个10/100/1000M自适应电口，4个SFP插槽(含4个SFP模块)，另有2个接口板卡扩展插槽（可扩展万兆端口），单电源。 |
| 部署模式 | 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求，支持旁路模式。 |
| 路由协议 | 所投产品必须支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式） |
| 所投产品必须支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于12种路由负载均衡方式，支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试（提供相关说明或证明材料） |
| 所投产品必须支持ISP路由负载均衡，最大可支持8条链路负载，支持自定义负载权重，支持基于优先级的ISP路由链路备份；支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试 |
| 地址转换 | 所投产品必须支持全面的NAT转换配置，包括包括一对一，一对多，多对一的源、目的地址转换，并至少支持FULL\_CONE模式和SYMMETRIC模式 |
| IPv6支持 | 所投产品必须设备接口支持配置IPv6地址，并可使用IPv6地址管理设备；支持IPv6手动及自动的IP/MAC探测及绑定； |
| 所投产品必须支持IPv6下静态路由及策略路由、动态路由，动态路由应包括RIPng、OSPFv3、BGP4+ |
| 所投产品必须支持针对IPv6流量通过HTTP、HTTPS实现Web认证，用户身份信息可存储在本地或Active Directory\Radius\TACACS+\POP3等第三方服务器；通过HTTPS实现Web认证必须支持使用本地CA颁发的证书同时使用证书验证客户端身份（提供相关说明或证明材料） |
| 高可靠性 | ▲所投产品必须支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA高可靠性部署支持接口联动，某个端口失效（DOWN），属于同一接口组中其他端口都会进入失效状态（DOWN）；HA高可靠性部署支持配置接口权重；支持链路探测（提供相关说明或证明材料），系统支持双机热备功能，要求支持路由和透明模式下的“主-备”、“主-主”模式，要求系统必须具备自主研发的多防火墙负载均衡技术，须提供相应证明文件 |
| 虚拟防火墙功能 | 所投产品必须支持将物理防火墙资源，如会话数、安全策略数、源NAT数、目的NAT数，日志存储数量以保留值及最大值的形式自动分配。 |
| 所投产品必须支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计； |
| 应用识别与控制 | 所投产品必须支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类（提供相关说明或证明材料） |
| 所投产品可直观展示不同风险等级的应用在1天（24小时）或一周（7天）内传输流量的绝对数值及占全网流量的百分比。 |
| 用户识别与认证 | 所投产品必须支持基于用户的访问控制，可与LDAP/Radius/证书/Active Directory/TACACS+/POP3等用户认证系统联动 |
| 支持二层MAC地址IP地址绑定；支持跨三层MAC地址IP地址绑定 |
| 文件过滤 | 所投产品必须支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤，应用至少包含即时通讯、常用协议、文件共享、论坛、博客、网页邮件五种分类； |
| 所投产品必须支持上传、下载、双向的文件内容过滤；内容过滤支持手工及文件批量导入两种方式进行敏感信息定义；内容过滤至少支持html、doc、docx、xls、xlsx、ppt、pptx、chm、7z等30种常见文件类型；文件类型识别基于文件特征而非扩展名，更改文件扩展名后仍可有效识别 |
| 网络攻击防护 | 所投产品必须支持基于不同安全区域防御DNS Flood、HTTP Flood攻击，并支持警告、阻断、首包丢弃、TC反弹技术、NS重定向、自动重定向、手工确认等多种防护措施（提供相关说明或证明材料） |
| 所投产品必须支持可配置阈值的基于安全域或基于二层接口局域网广播防护，防止局域网内广播和多播数据包泛滥 |
| 病毒防护 | 所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀 |
| 所投产品必须支持对最多6级的压缩文件进行解压查杀 |
| 所投产品必须支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀（提供相关说明或证明材料） |
|
| 入侵防御 | 所投产品必须支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的漏洞防护 |
| 所投产品必须支持在设备漏洞防护特征库直接查阅攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息；（提供相关说明或证明材料） |
| 所投产品的漏洞防护特征库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息；（提供相关说明或证明材料） |
| 所投产品必须支持间谍软件防护功能，同时将间谍软件特征库分类，至少包括木马后门、病毒蠕虫、僵尸网络等三种分类;支持在防火墙间谍软件签名库直接查阅攻击的名称、严重性、描述等信息；间谍软件防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的间谍软件防护 |
| 所投产品必须支持自定义TCP、UDP、HTTP协议的漏洞特征，漏洞特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配，并可自定义漏洞的源、目的端口范围；同时可标识自定义漏洞的CVE编号或CNNVD编号。 |
| 所投产品必须支持自定义基于TCP、UDP、HTTP协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围 |
| 网络异常感知 | 所投产品必须支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断（提供相关说明或证明材料） |
| 所投产品必须支持基于主机或威胁情报视图，统计网络中存在安全风险的主机数量以及对应的风险等级，至少可查看遭遇风险的时间、威胁类别、情报来源、威胁简介、失陷主机IP、用户名、资产等信息 |
| 安全事件分析 | 所投设备必须提供关联分析面板，可将Top应用、Top威胁、Top URL分类、Top源地址、Top目的地址等信息关联，并支持以任意元素于为过滤条件且不少于35个维度进行数据钻取（提供相关说明或证明材料） |
| 所投设备必须支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为（提供相关说明或证明材料） |
| 策略与处置 | 所投设备可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项。 |
| 所投设备必须支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索，支持策略的复制、调序、查询 |
| 所投产品必须支持基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括1天、7天、30天、90天、永久等； |
| 运维管理 | 所投产品必须支持双系统备份，且在系统切换中可实现配置的自动迁移；可记录不同时间点的历史配置文件。 |
| 协同防御 | 所投产品必须支持与云端联动，至少实现病毒云查杀、URL云识别、应用云识别、云沙箱、威胁情报云检测等功能（提供相关说明或证明材料）▲所投产品必须支持与招标单位中配置的桌面杀毒或终端管理软件联动，实现基于终端健康状态的访问控制，增强防火墙对木马特征的识别能力（投标文件需要提供能够体现上述功能及配置说明或证明材料）； |

**（2）上网行为管理设备（1台）**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 性能配置 | 产品为标准1U机架式设备，标配6个千兆电口，2个千兆光口，并含2个高速USB2.0接口，1个RJ45串口，性能配置：最大并发连接数≥150,000；用户规模≥1500人；并发带宽≥400M；每秒新建连接数≥4000；硬盘≥1TB；支持BYPSS |
| 集中管理 | 多台设备支持通过统一平台集中管理、集中配置等； |
| 部署方式 | 要求设备支持网关模式，支持NAT、路由转发、DHCP等功能；支持网桥模式，以透明方式串接在网络中；支持旁路模式，无需更改网络配置，实现上网行为审计；支持两台及两台以上设备同时做主机的部署模式； |
| IPv6支持 | 支持部署在IPv6环境中，其所有功能（认证、应用控制、内容审计、报表等）都支持IPv6 |
| IPsec VPN | 必须具有IPSec VPN远程加密访问和连接的模块，并能提供IPSec VPN客户端授权远程接入访问； 支持配置主备线路组和流量分配模式的多线路选路策略； |
| 链路负载 | 为了提高出口多链路利用率，要求支持按剩余带宽、带宽比例、平均分配、前面优先的方式进行多链路负载。支持使用VPN做专线备份，支持链路故障检测；  |
| 终端管理 | 支持终端调用管理员指定脚本/程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等； 支持检测windows重要补丁的安装情况，并反馈检测结果；  |
| 系统识别：支持识别终端操作系统版本、系统补丁安装情况；进程识别：支持识别终端系统后台运行的进程信息，防止间谍软件的运行； |
| 业务需要 | 为减少短信费用投入，要求设备支持微信身份验证，用户可以通过微信“扫一扫”、关注公众号等操作获取上网权限，后台能够记录下用户微信的ID，支持与第三方微信平台对接，无需修改第三方平台代码 |
| 为满足访客PC的简易接入授权，访客终端接入无线网络后，终端自动弹出二维码页面，审核人通过手机扫描访客终端二维码，添加备注信息，访客即可完成上网，同时设备记录访客备注信息、接入终端MAC以及审核人帐号。（提供相关证明材料） |
| 对私接无线上网的行为管理，要求设备能自动发现网络中通过无线上网的热点和移动终端的IP和终端类型，匹配管理员配置的热点信任列表，对信任列表外非法接入的热点和终端能够进行阻止上网，支持冻结用户IP，并通过邮件形式告警通知管理员，支持显示以IP或用户名的维度统计一段时间内的趋势图。 |
| 为确保我单位不会通过SSL加密内容发生通过互联网出口泄密事件，要求设备必须能够识别并过滤SSL加密的钓鱼网站、金融购物网站；识别和审计加密的邮箱（如GMAIL）等； |
| 针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向web访问质量检测（提供相关证明材料） |
| 应用识别规则库 | 支持根据标签选择应用，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖6大类；此外可根据我单位需求自定义标签，根据标签做应用控制。 |
| 应用控制 | 设备内置应用识别规则库，支持超过6700条应用规则数，支持超过2900种以上的应用，1000种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率； |
| URL访问及关键字控制 | 要求设备内置海量的URL地址库，可根据访问URL的网页关键字进行过滤控制，特别对于SSL加密的网页、论坛、BBS上的发帖行为也需要支持关键字过滤控制 |
| 流控黑名单 | 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中 |
| P2P智能流控 | 要求设备有效抑制如迅雷、ppstream等P2P应用带宽，通过抑制可看到出口上下行带宽的明显改善。（提供相关证明材料） |
| 移动APP审计 | 支持常见论坛（天涯社区、猫扑社区、百度贴吧、新浪论坛、搜狐社区等）、微博（新浪）、新闻评论类（腾讯新闻、网易新闻、搜狐新闻、新浪新闻）的移动APP内容审计 |
| IM审计 | 支持对QQ（客户端版本）、阿里旺旺、万德（Wind）、路透等应用的聊天，群聊天等内容的审计 |
| SSL加密内容审计和过滤 | 支持识别并过滤SSL加密的钓鱼网站、金融购物网站、非法网站等，同时支持SSL硬件加速卡解密，从而可提高SSL全流量解密性能；（提供相关专利说明或证明材料并加盖厂商公章） |
| 加密证书自动分发 | 审计SSL网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。解决管理员给每台PC单独安装证书的问题 |
| 网络整体状况报表 | 设备能根据管理者自定义的风险行为特征自动挖掘并输出离职风险、泄密风险、安全风险、工作效率风险、法律风险智能报表 |
| 单用户行为分析 | 针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等） |
| 病毒查杀 | 必须具有防火墙功能模块；设备可扩展支持业界知名杀毒引擎必须能查杀网页、Email、FTP等流量中的病毒；支持能查杀RAR，Gzip等压缩包中的病毒； |
| 数据中心 | 要求设备必须支持将审计数据备份到外置数据中心，实现海量存储；必须支持通过USBKEY方式对数据中心管理员进行身份验证，确保我单位核心数据不会外泄 |
| 外置数据中心虚拟化 | 为了保障日志平台运行稳定且具备高可用性，支持自有品牌的免费服务器虚拟化软件（提供软件著作权证书）与外置数据中心联动。 |
| 资质要求 | 为保证软件开发质量，具备CMMI L5认证证书产品应具备相当的技术认可度，最近两年产品曾入围Gartner SWG魔力象限（提供相关证明材料）国家标准《信息安全技术信息系统安全审计产品 技术要求和测试评价方法》的主要起草单位；（提供相关证明材料） |

**（3）WEB安全防护系统（1台）**

|  |  |
| --- | --- |
| **技术指标** | **规格要求** |
| **硬件****规格** | 1U专业机架式硬件设备，系统硬件采用全内置封闭式结构，产品稳定可靠性高 |
| 产品必须为专业性WEB应用防火墙设备，而非NGAF、NGFW、UTM设备 |
| 至少具备6个10/100/1000自适应电口，产品至少具备2个扩展槽，支持扩展板卡 |
| 设备采用单电源，配置有USB、console接口 |
| 产品应具备硬盘存储日志系统，硬盘容量≥1000GB |
| 硬件内置有fail-open模块，至少具备2组fail-open接口，产品出现故障时，能自动转变成通路，不影响流量正常传输 |
| 支持液晶面板实时显示，包含IP地址、登陆用户、CPU、内存、session等详细信息 |
| **性能指标** | 至少1Gbps网络吞吐量 |
| http最大并发为24万 |
| http新建速率大于5000/s |
| **部署模式** | 产品具备支持旁路部署，通过反向代理方式对Web流量进行过滤防御 |
| 产品具备支持镜像分析数据并实现旁路阻断功能，产品具备专门的阻断接口设置（提供相关说明或证明材料） |
| 产品具备支持ARP协议，对静态、动态ARP进行绑定 |
| **网络自适应** | 产品具备支持IPv4和IPv6双协议栈流量过滤 |
| 产品具备符合RFC标准，支持HTTP和HTTPS协议合法性进行验证，提供HTTP协议防护功能 |
| 产品具备支持对SSL（HTTPS）加密会话进行分析 |
| **服务器环境** | 产品具备支持对HTTP 0.9/1.0/1.1协议过滤 |
| 产品具备支持对虚拟机中的任意数量网站进行防护，使多个虚拟机共用一个IP地址 |
| 产品具备支持对负载均衡服务器任意数量网站进行防护，内置有负载均衡算法，包含轮询、Hash算法 |
| 产品具备支持代理服务器模式，支持HTTP、HTTPS代理模式，提供针对后端服务器的代理模式 |
| **Web安全** | 产品具备内置有标准特征库，并且可以自定义特征，定义检查方向、严重级别、Web攻击特征等信息 |
| 产品具备支持自定义拦截防御页面的标题、页面内容等相关设置项（提供相关说明或证明材料） |
| 产品具备支持SQL注入、跨站脚本、防爬虫、扫描器、信息泄露、溢出、协议完整性等至少7种知识库展示说明（提供相关说明或证明材料） |
| 产品具备支持HTTP协议校验细粒度规则检测，至少提供20种HTTP协议校验策略参数，其中要包括Cookies、Response、Range等策略参数 |
| 产品具备对HTTP协议检验参数提供参数值设置、并提供3种严重级别分类和至少5种处理动作设置 |
| 产品具备支持HTTP访问控制细粒度规则检测，至少提供14中HTTP访问控制路测参数，其中要包含GET、Post、Head、Delete等策略参数（提供相关说明或证明材料） |
| 产品具备对HTTP访问控制参数提供优先级设置、并提供3种严重级别分类和至少5种处理动作设置（提供相关说明或证明材料） |
| 产品具备独立的防盗链规则，应支持Referer和Cookie检测方式（提供相关说明或证明材料） |
| 产品具备防跨站请求伪造功能，应支持Get、Post检测方式 |
| 产品具备扫描陷阱功能，防御漏洞扫描提供针对恶意扫描的防御效果 |
| 产品具备非法上传防护，需支持根据文件类型、MIME类型及真实文件识别等策略参数 |
| 产品具备非法下载防护，可以根据文件大小、MIME类型，灵活定义下载限制策略，限制用户非法获取网站的关键数据 |
| 产品具备敏感信息检测功能，用户可以自定义检测敏感信息，并提供替换功能，替换信息可以根据用户需求自行定义（提供相关说明或证明材料） |
| 产品具备弱密码检测功能，提供用户名、密码字典检测机制（提供相关说明或证明材料） |
| **Syslog****日志** | 产品具备Syslog协议接口，提供字符串和JSON格式的日志外发功能 |
| 产品具备攻击、访问、安全情报、流量日志类型的Syslog日志外发功能 |
| **审计及分析** | 产品具备至少8种日志审计，包含备份、审计、访问、攻击、篡改等分类日志记录 |
| 产品具备日志备份功能，提供手工、自动备份模式 |
| 产品具备日志恢复功能，提供备份自动恢复还原点设置 |
| 产品具备对CDN、XFF的IP地址的日志记录功能，为网站攻击溯源提供技术依据（提供相关说明或证明材料） |
| 产品具备访问日志数据分析功能，提供访问源、源地域、访问域名的概况和趋势效果展示（提供相关说明或证明材料） |
| 产品具备攻击日志数据分析功能，提供攻击类型、攻击源IP、源地域、被攻击域名的概况和趋势效果展示（提供相关说明或证明材料） |
| 产品支持自动生成报表功能，提供系统信息、设备环境、业务统计等报表模板 |
| **账户管理与认证** | 产品具备三权分立管理，必须有管理员账户、审计管理员、配置管理员 |
| 产品具备虚拟化管理划分，虚拟多个系统进行设备划分管理 |
| **管理界面** | 产品具备超时重新认证机制并能够定义用户认证尝试的最大允许失败次数 |
| 产品具备SSL的Web页面、SSL、ping等方式，并进行相应管理限制 |
| 产品具备中、英文管理界面 |
| 产品具备HTTPS协议管理，可以通过界面修改Web GUI端口（例如443可改为4431） |
| **系统诊断** | 产品具备系统CPU、内存、硬盘、并发连接数等信息，以及系统时间 |
| 产品具备远程技术支持信息提取，辅助技术支持人员快速排查问题 |
| 产品具备SSH远程连接设置，无需登录第三方设备即可实现设置SSH远程自动连接支持服务 |
| 产品具备升级功能，针对系统、特征库提供升级保障 |
| **冗余系统** | 产品具备冗余系统备份机制，升级或运行中出现软件异常，可自动切换至备份系统保障设备正常运行（提供相关说明或证明材料） |
| **产品资质** | 产品具有《国家信息安全测评信息技术产品安全测评证书（EAL3+级）》 |

**（4）数据库审计设备（1台）**

|  |  |
| --- | --- |
| **技术指标** | **规格要求** |
| 规格性能 | 事件处理12000条/秒，内置4TB磁盘存储空间。标准1U机箱，单电源；主机带6个千兆自适应电口（1个管理口，5个侦听口），1个Console口，支持液晶屏。3年保修 |
| 审计范围 | 审计包括包括MS SQL Server、Oracle、DB2、Sybase、MySQL、Informix、达梦、Postgresql等在内的多种数据库 |
| 支持审计HTTP/HTTPS协议的URL、访问模式、cookie、页面内容、Post内容 |
| 数据库审计 | 支持Cache数据库集成工具terminal、portal、studio、Sqlmanager、MedTrak工具的审计，其中Portal能审计到sql语句、查询Global、返回结果，Terminal能审计到M语句和返回结果 |
| 中间件的支持，支持COM、COM+、DCOM组件 |
| 数据库安全 | 支持对SQL注入、跨站脚本攻击等web攻击的识别与告警 |
| 审计策略 | 支持数据库语句执行时间、语句执行回应、最大操作语句长度等作为分项响应条件 |
| 数据库审计策略支持数据库客户端软件名称、数据库名、数据库表名、数据库字段名、数据库返回码作为响应条件 |
| 支持超长操作语句审计，针对传统型数据库，支持3万字节的审计而不截断 |
| 审计查询 | 审计数据支持18种以上查询条件，可支持按数据库操作命令（包括select、create等14个命令）、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、、客户端MAC、客户端IP、客户端端口、、会话ID、关键字、时间（包括开始、结束日期）等为条件进行查询,还可以提供客户端操作系统主机名、客户端操作系统用户名、客户端进程名等信息 |
| 实现对所有违规事件出现频率进行图形化的汇总统计分析，并提供对汇总结果的实时查询功能； |
| 可以对客户端使用的程序、使用频率进行图形化排名展示 |
| 审计安全 | 审计结果隐秘设置，通过\*号对审计结果中的重要信息进行隐秘处理，防止非法权限查看 |
| 系统本身具备能发现未知仿冒进程工具、防范非法IP地址、防范暴力破解登录用户密码、设置系统黑白名单等安全功能 |
| 管理员登陆支持静态口令认证，支持密码的复杂性管理，比如大小写、数字、特殊字符、长度等 |
| 能够对连续失败登陆进行自动锁定，锁定时间可设置 |
| 配置管理 | 采用B/S管理方式，全中文界面 |
| 提供系统升级功能，能够通过升级包的方式实现升级 |
| 提供审计数据管理功能，能够实现对审计数据的自动备份、手动备份，支持增量、全量备份方式 |
| 提供设备自身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）日志审计设备（1台）**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 资质 | 产品资质 | 计算机软件著作权登记证书、软件产品证书、销售许可证 |
| 产品专利 | 已获得数种专项专利，并提供可查询专利号 |
| 系统配置 | 产品架构 | 产品为软硬件一体化的日志审计系统；无需用户另行提供服务器、 操作系统、数据库、防火墙软件、及用户手动升级系统补丁 |
| 部署方式 | 提供单点接入模式，设备部署不影响原有网络结构 |
| 管理结构 | B/S架构 |
| 日志生命周期管理 | 包括数据库日志采集、审计分析、存储备份功能 |
| 系统支持 | 支持系统维护行为审计 |
| 支持支持外部存储 |
| 支持Raid |
| 硬件配置 | 硬件规格 | 专用硬件平台， 1U |
| 处理器 | 多核超高性能处理器 |
| 接口配置 | 千兆电口6个；支持扩展 |
| 数据存储 | 32G内存，物理磁盘空间≥4T支持Raid架构以保证数据可靠性 |
| 日志存储量 | 10亿条 |
| 日志吞吐量 | 3000EPS |
| 使用许可 | 含200个审计许可，最大可支持600个审计设备 |
| 产品功能 | 日志收集 | 协议类型 | 支持标准的syslog协议进行日志的采集，通过指定的syslog监听端口与告警接收级别进行设置所要接收的日志类别 |
| 管理方式 | 支持日志信息的统一管理，系统通过统一集中的日志管理展现 |
| 支持设备 | 支持上百种设备及应用日志 |
| 日志存储 | 压缩存储 | 原始日志数据进行高效压缩存储灵活设置系统日志存储空间上限，达到告警上限提示管理员及时处理，达到删除上限会自动删除最旧日志释放空间 |
| 原始日志长期存储 | 原始日志支持长期存储存储策略可以通过管理平台配置，可以针对不同的日志源制定不同的存储策略 |
| 存储空间监控 | 支持存储空间动态监控，超过阀值进行告警支持从存储空间、存储时间多维度进行动态监控 |
| 存储位置可定义 | 支持自定义存储位置（磁盘阵列、SAN、NAS等外部存储网络）以获取超大存储空间 |
| 数据备份与恢复 | 支持对系统内关键数据的自动备份与恢复功能，备份方式为实时手动备份，保证客户数据的完整性与数据迁移的便捷性 |
| 日志传输 | 日志可加密压缩传输，保证数据的完整性和机密性 |
| 日志转发 | 可根据转发条件，将采集范式化后的数据转发到其他的目标地址 |
| 支持加密压缩方式转发，定时转发 |
| 日志查询 | 日志查询 | 支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索等 |
| 支持以日志类型、时间范围及条件字段快速检索过滤 |
| 将备份的日志信息导入系统后进行日志检索查询 |
| 支持高级检索以多条件组合方式查询，可以将每一个日志字段作为查询条件进行查询 |
| 支持查询结果导出 |
| 格式归一化 | 支持将不同设备所产生的不同格式的难以理解的日志数据进行统一格式化处理，提炼出有用信息清晰、明确的展示给管理者 |
| 管理平台 | 日志源管理 | 管理员可以对日志源进行查看、添加、编辑、删除以及启\禁用的操作 |
| 支持主流网络设备、服务器、操作系统、数据库等 |
| 基本功能 | 支持日志源类型的添加，系统支持网络设备、操作系统及数据库类型日志源设备 |
| 支持通过操作栏对已添加的日志源进行黑白名单设置、编辑、删除操作，支持批量删除已添加日志源设备 |
| 支持通过类别查询已添加的日志源信息 |
| 支持全网日志级别数量统计展示图，支持全网日志数量时间分布展示图 |
| 用户管理 | 支持用户信息新增，可通过设置权限控制角色访问页面菜单，支持新建用户设置ip限制功能 |
| 系统支持通过类别快速查询用户信息支持通过操作栏对用户进行账号信息锁定解锁、查看、编辑、删除操作 |
| 系统具有防恶意暴力破解账号与口令功能口令错误次数可设置，超过错误次数锁定，锁定时间可设置 |
| 系统支持三权分离管理模式 |
| 可自定义的事件库 | 系统支持事件库的自定义设置，通过事件库对某类事件进行告警设置，告警方式可通过邮箱推送，已添加事件库的批量及单个删除，支持对已添加事件库进行查看、编辑 |
| 资产管理 | 支持对常见的网络设备、主机设备、数据库等日志源接收设置，通过统一页面进行管理展示 |
| 告警响应 | 实时告警显示日志收集与分析系统最新的告警信息系统支持告警历史数据的统一展现通过新增告警设置可自定义告警规则，方便用户实时管理规则告警支持邮件、短信、屏幕、微信告警 |
| 磁盘容量告警 | 系统支持自定义磁盘容量值，当磁盘容量达到预先设定的阈值时触发告警，告警方式可通过邮件配置发送相应的管理人员，有效防止由于磁盘容量而带来的系统异常 |
| 报表分析 | 支持动态/静态（日报、周报、月报）两种系统生成方式  |
| 支持报告的邮件转发、生成提醒功能，支持多人邮件接收 |
| 支持导出html、Excel、PDF |
| 报表管理 | 管理员可以查看系统内置的各种类型的报表 |
| 用户可以按照自己的需求制作个性化的报表 |
| 可以定期定时发送报表到指定的邮件账户，满足了用户有规律的接收报表、定期了解设备情况的需求 |
| 系统自身安全 | 系统内置安全防火墙，可设置防火墙策略 |
| 系统状态实时监视 | 管理中心状态监视 | 可以通过管理平台首页可以清晰查看到单日安全事件概况、实时告警信息 |
| 审计中心状态监视 | 可以实时查看审计中心主机的CPU、内存以及磁盘等的使用情况 |
| 其他 | 产品服务 | 为保证项目的顺利实施与信息安全保障能力，须具备中国信息安全认证中心颁发的《信息系统安全集成服务资质证书》、《信息安全风险评估服务资质证书》，并通过ISO27001信息安全管理体系认证 |

**（6）负载均衡设备（1台）**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 配置要求 | 吞吐量≥ 5Gbps，并发连接数≥ 300万，4层新建连接数CPS ≥18万，7层新建连接数RPS≥9万，默认内存≥4GB，硬盘≥240GB SSD，网络接口≥ 6个千兆电口，≥2个千兆光口，机架式。 |
| 业务要求 | 必须独立专业负载设备，非插卡式负载均衡设备支持路由、旁路、三角传输等方式单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使用状态，无需额外购买相应授权。支持轮询、加权轮询、按主机加权轮询、加权最小连接、按主机加权最小连接、动态反馈、最快响应、最小流量、加权最小流量、按主机加权最小流量、带宽比例、哈希、主备、首个可用、优先级等算法支持基于URL的链路调度功能，内置不少于1000条的国外URL网址库，无需手动导入并支持自动更新，管理员可查看并进行编辑。可根据URL将访问国外网站的请求调度到指定线路。支持基于应用协议的智能选路，能对网银、游戏、视频等流量进行调度（提供证明材料并加盖厂商公章）支持路由配置向导功能，引导管理员按照所期望的出口链路使用效果，完成链路负载策略的配置支持IPv6双栈模式，支持NAT46、NAT64、NAT66等协议转换在三明治架构下，支持跨设备（如防火墙、IPS、行为管理等）对后端的设备进行健康状态监控（透明监视），同时支持Ipv4和Ipv6（提供相关说明或证明材料）IPv6改造方案能够解决天窗问题，支持一条策略匹配多个外链网站，同时外链和网站子链发生修改时支持自动识别并做主动修改，不允许通过人工解析配置的方式解决天窗问题支持非对称式部署的TCP协议优化技术，提升远端用户访问应用服务的速度。无需安装任何插件和软件，不受操作系统类型、浏览器版本等兼容性因素限（提供相关说明或证明材料）对某种编程语言（如lua）实现自定义的流量编排，对TCP、SSL、HTTP和HTTPS等类型的流量进行分发、修改和统计等操作。 |
| 功能要求 | 支持链路负载投屏展示，能够分别基于链路监测、应用选路和ISP流量进行投屏展示分析。链路监测展示链路的健康状态、上下行带宽、总带宽、新建连接数、并发连接数和吞吐量；应用选路展示基于应用分类选择相应链路的示意图；ISP展示基于运营商分类选择链路的示意图。（提供设备操作界面相关证明材料）SLB能够通过健康检查来获取后端服务器状态，同时将服务可用性、设备CPU、新建并发吞吐等数据上报GSLB，设备之间的联动使得GSLB能根据链路和服务器两者的综合状态实现智能切换，为用户选择最优的数据中心和服务器分配方式。支持静态IP和PPPOE两种线路接入方式。支持大数据输出功能，输出必须包括客户端IP、x-forwarded-ForIP、访问时间、访问IP、访问URL、响应时间和资源大小。节点支持域名和IP两种形式，支持自定义DNS查询间隔。支持后端服务不可用时主动关闭连接，保证客户端访问的连续性支持DNS内网记录，包含A、CNAME、MX和TXT等类型；支持多种链路检测方法，能够通过PING、TCP、HTTP等方式监控链路的连通性支持基于管理员自定义的时间计划来进行出站访问的流量调度分发。支持常见的主动式健康检查功能，提供基于SNMP、ICMP、TCP/UDP、FTP、HTTP、DNS、等多种类型的探测判断机制支持用户自定义方式的健康检查，支持多种编程语言（如Python、Java等），用户可根据节点运行的实际业务流程来编写代码，检查业务处理逻辑是否正常。（提供相关说明或证明材料）具备会话保持：支持源IP、Cookie（插入/被动/改写）、HTTP-Header、SSL Session等多种会话保持机制支持图片优化技术，通过对图片格式的转换，减少传输流量，提升web页面加载速度。支持被动式健康检查，可根据对业务流量的观测采样；对常规HTTP应用可配置基于反映URL失效的HTTP响应状态码的观测判断机制，对于复杂应用可配置基于RST关闭连接和零窗口等异常TCP传输行为的观测判断机制。支持面向服务器健康度的弹性调控机制，可通过监控业务流中的TCP传输异常来衡量服务器节点的有效性，尝试对性能不足的服务器临时开启过载保护，动态调节服务器的负载。服务器负载状态支持投屏展示，能够显示设备的电源状态、风扇转速、磁盘温度、CPU和内存占用率、新建连接数、并发连接数、SSL新建和SSL吞吐数据、压缩优化和缓存优化数据；业务的健康状态、上下行流量、每秒请求数、健康状态 支持实时漏洞检测功能，通过对实时流量进行安全性分析来评估业务系统的漏洞风险 |
| 资质和售后服务 | 所投产品生产厂商具备CMMI 5级资质。设备生产商的负载均衡类产品入选Gartner应用交付控制器（ADC）魔力象限报告，提供7×24小时400电话支持 |

**（7）网络防毒墙（1台）**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 硬件参数 | 产品类型 | 硬件, 产品必须为国有品牌，必须专业反病毒厂商产品，拥有自主知识产品 |
| 产品构架 | 要求是X86平台，具有多重病毒过滤技术、虚拟化病毒分析技术等应用基础、同时支持ipv4和ipv6协议 |
| 多出口 | 要求支持多路链路出口 |
| 工作环境 | 温度0-40摄氏度湿度20-90%非凝结 |
| 平均无故障间隔时间 | ≥50，000小时 |
| 产品规格 | 2U标准机箱 |
| 硬件平台 | 要求双路多核专业网安硬件平台，保障设备处理性能 |
| 网络接口 | 6个10/100/1000BASE-T接口（支持2对Bypass接口）;支持Bypass光口，要求支持万兆和千兆光口、电口灵活扩展，最多可扩展12个光口 |
| 电源要求 | 要求冗余电源 |
| 性能参数 | 最大吞吐 | 8Gbps |
| 杀毒吞吐 | ≥3Gbps |
| 最大并发数 | 5,000,000 |
| 新增并发数 | 70,000 |
| 系统功能 | 产品成熟度 | 要求产品采用国内领先的检测过滤技术，并具有专门的安全操作系统 |
| 部署模式 | 要求支持旁路监听模式、透明模式等灵活的部署方式，产品即插即用；旁路监听模式支持多端口监听；透明模式支持多路透明网桥；（提供相关证明材料） |
| 管理方式 | 要求支持HTTPS、SSH、console方式，支持防毒墙集中管理功能。 |
| 帐户管理 | 要求支持指定管理员管理设备（绑定IP）；支持管理员账户超时、锁定等安全保护 |
| 备份与恢复 | 要求对系统配置进行备份，恢复备份配置、恢复系统默认值 |
| 病毒过滤技术 | 病毒监测能力 | 要求具有针对国内及全球病毒监测网络，具备新病毒及时发现、处置能力及专业技术资源，保障对新病毒的有效拦截及具备先进的病毒分析技术实力 |
| 杀毒引擎 | 要求具有国内独立自主产权杀毒引擎，专业的网关病毒过滤引擎，保障防毒墙在网关过滤病毒的效率及性能 |
| 数据并行处理技术 | 要求具有并行数据处理分析技术，可以完成多链路、高流量环境的病毒过滤 |
| 病毒库特征码 | 要求具有针对国内用户的病毒库，病毒库特征码≥200万 |
| ▲支持协议及多端口过滤技术 | 要求支持SMTP、POP3、FTP、HTTP和SAMBA协议的双向传输病毒过滤, 并可对SMTP、POP3、FTP、HTTP等协议通过不同端口传输的数据同时具有病毒过滤功能（提供相关说明或证明材料） |
| 扩展病毒分析技术 | 要求支持对可执行、库、邮件、脚本、DOS可执行、图片格式病毒查杀 |
| 加壳病毒分析 | 要求必须支持虚拟化病毒分析等脱壳技术，对加壳病毒具备识别及阻断能力 |
| ▲病毒过滤策略 | 要求支持多层压缩文件中的病毒过滤，可定制压缩层数和不查杀文件类型;支持对病毒文件进行隔离和拥有对未知病毒识别及阻断能力（提供相关说明或证明材料）） |
| 恶意网站拦截 | 要求恶意网站URL数量≥2000万 |
| 病毒库升级 | 要求支持在线自动、手动方式升级，局域网升级 |
| 要求在国内有自主的分布式病毒库升级服务器，保障防毒墙设备病毒库升级的可持续性 |
| 入侵防御 | 支持对各种蠕虫病毒攻击的防御。 |
| 双归属链路 | 要求支持对双归属链路环境的支持，可以满足非对称路由网络环境的需求。 |
| URL数据同步 | 要求双归属链路中的不同链路的两台墙之间支持URL数据同步功能。 |
| 非代理应用层杀毒技术 | 要求保证不改变经过防毒墙数据的任何特征，做到“透明代理”更加透明。 |
| 半连接杀毒技术 | 要求具备对网络中半连接的数据进行病毒查杀的功能。 |
| 白名单配置管理 | 要求支持自定义URL白名单，对访问网址不进行病毒过滤 |
| 要求支持自定义IP地址(范围)白名单，对特定的IP地址不进行病毒过滤 |
| 要求支持自定义邮件地址或邮件域白名单，对特定邮件地址或域不进行病毒过滤 |
| 单位安全管理 | 单位评价 | 单位评价功能通过近期病毒过滤的数据统计，得出各单位的病毒危害度及未来趋势，为内部单位病毒情况提供有利的数据手段。（提供相关说明或证明材料） |
| 单位分析 | 能够对每个单位病毒过滤情况进行统计，分析得出每个单位的传毒次数、传毒种类、传毒主机数等。 |
| 日志管理 | 日志管理 | 要求提供系统日志、病毒日志、隔离日志、管理日志等 |
| 日志报表 | 要求对详细病毒日志查询及日志统计，并支持日、周、月、季、年、自定义等日志报表功能，可发送日志信息给管理员 |
| 远程日志 | 要求支持SYSLOG、MYSQL远程日志服务 |
| 防毒墙资质 | 产品资质 | 具有公安部安全产品销售许可证书；具有计算机软件著作权登记证书； |
| 制造商资质 | 具有向国内个人及各行业客户提供信息安全领域反病毒、安全防范软件设计开发和技术支持服务相关的信息技术服务的信息技术服务管理体系认证证书。具有与信息安全领域反病毒、安全防范软件设计开发和技术支持服务相关的信息安全管理活动的信息安全管理体系认证证书。具有信息安全领域杀毒、安全防范等软件系统的设计开发和服务的质量管理体系认证证书。 |

**（8）VPN设备（1台）**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 性能配置 | 专业VPN设备，非插卡或防火墙带VPN模块设备；产品为标准1U机架式设备，需满足多核X86架构，标配4个千兆电口，并含2个高速USB2.0接口，1个RJ45串口，吞吐量≥500Mbps，并发会话数≥600,000，SSLVPN最大加密流量≥200Mbps，IPSecVPN最大加密流量≥85Mbps，本次VPN设备需提供100个SSL VPN接入授权，100个钉钉应用封装授权 |
| 部署方式 | 支持网关模式、单臂模式部署两种方式；支持虚拟化方式部署 |
| 基本特性 | 同时支持IPSec VPN、SSLVPN两种VPN； |
| 设备支持多种终端系统，如windows10、mac OS X El Capitan、ios9.x等及以下版本，使用包括IE11及以下版本或其他IE内核的浏览器，以及非IE内核浏览器，如Firefox，Safari，Google Chrome，Opera登录SSLVPN系统，登录后可完整支持各种IP层以上的B/S和C/S应用 |
| 产品应支持的密码算法包括：AES、DES、3DES、DH、RSA、RC4、MD5、SHA1； |
| 易用性 | 可支持虚拟门户功能，在一台设备上配置不同的域名、IP，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果；  |
| 支持断线重连自动技术，防止用户关闭浏览器或无线网正常切换时VPN隧道断开。支持客户端永久在线功能，对于无人值守的设备可以设定永久在线。 |
| 产品应提供环境检测、自动修复工具，支持对Windows的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响SSL VPN的使用，减轻运维工作。（提供相关说明或证明材料） |
| 终端安全 | 产品必须支持防中间人攻击，产品可在用户登录SSLVPN时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象。 |
| 支持客户端注销后自动清除所有缓存、Cookies、浏览器历主从认证账号绑定史记录、保存的表单信息，实现零痕迹访问。 |
| 支持VPN专线功能，可配置用户在接入SSL VPN的同时，断开与Internet其他连接  |
| 提供HTTPS驱动病毒查杀工具，支持对Windows环境下的HTTPS拦截监听的驱动病毒进行扫描查杀，避免因为HTTPS驱动病毒导致无法正常接入和使用SSL VPN（提供相关证明材料） |
| 支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统 |
| 身份认证 | 产品必须支持Local DB 、USB KEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式；可针对用户/用户组设置认证方式的与、或组合； |
| 支持与阿里钉钉、企业级微信绑定，实现其内置OA的安全接入（提供相关证明并加盖厂商公章） |
| 设备内部必须支持自建CA中心，便于数字证书认证平台搭建；支持与第三方CA进行结合认证，支持CRL证书撤销列表；单台VPN设备可扩展同时支持5套以上CA根证书 |
| 高速性 | 支持利用网页进行动态寻址的方法，客户端直接根据速度探测实现用户端接入线路的自动优选,用户通过访问寻址代理页面（简称Webagent页面）自动寻找VPN设备IP(非DDNS),该方法不必单独注册域名或占用IP地址。 |
| 支持非对称式部署的传输协议优化技术（单边加速），不用在用户终端上安装任何插件和软件，即可提升用户访问应用服务的速度。（提供相关说明或证明材料） |
| 支持针对不同的web页面进行数据优化，支持动态压缩技术，针对B/S资源支持WebCache技术，动态缓存页面元素，提高Web页面响应速度。支持流缓存技术，提高访问速度（提供相关证明材料） |
| 支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果 |
| 高管理要求 | 支持独立日志中心进行SSLVPN实时日志记录，支持Syslog（系统日志）服务器，将日志输出到syslog服务器中； |
| 为满足我单位多数据量的保存，保障日志平台运行稳定且高可用性，必须支持外置数据中心，同时免费提供自有服务器虚拟化软件（提供软件著作权证书）及3颗物理CPU授权。 |
| 稳定性、可扩展性 | 支持基于自组域简化部署VPN网络的方法，即当有多台设备处于VPN网络中时，通过连接任意节点的VPN设备，即相当于连入整个VPN网络； |
| 在负载均衡集群部署模式下，支持授权漂移，即当集群中一台设备宕机，该宕机设备中的并发授权自动迁移到其他正常的设备中，而无需额外购买授权。 |
| 产品必须支持经过集成的，基于Android IOS平台的第三方软件开发包（SDK），并实现基于Android IOS平台第三方应用软件（APP）代码量不超过20行。（要求提供代码Demo和企业证明）支持针对移动APP的VPN安全代码的自动封装，实现App应用的安全加固 |
| 防火墙 | 产品应具备基于状态监测技术的防火墙功能，能够抵抗常见的网络攻击，能够进行包过滤或WAN、LAN、DMZ口之间访问控制；产品必须支持对防火墙的过滤规则进行在线虚拟测试。  |
| 产品及企业资质 | 所投产品产商获得云安全最高级别认证资质CSA-CMMI5（提高证明材料）。（提供证书复印件） |
| 设备生产厂商需为国家密码管理局发布的《SSL VPN技术规范》起草单位之一（提供证明材料） |
| 提供SSL VPN。（提供证明材料） |
| 产品经过IPV6 Ready认证，并在全球IPV6测试中心官网可查 |

**（9）数据备份一体机（1台）**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 品牌 | 国产知名品牌，具有十年以上的销售历史，具有自主知识产品，在杭州设有常驻机构保障后续服务能力 |
| ▲基础架构 | 企业级多功能实时保护系统，基于设备底层IP-SAN数据块级保护设计（非TCP/IP协议），可以实现各种软、硬件故障保护及灾难性恢复，无备份时间窗口，保护过程中对生产业务系统无影响，配置连接设备所需的各种连接线缆及连接附件,提供iSCSI块协议保护（提供相关说明或证明材料） |
| 存储控制器 | 配置64位6核高性能处理器，XOR双ASIC运算芯片，双PCI-E总线设计。内部无线缆连接，非Windows内核设计(杜绝网络病毒攻击) |
| 缓存 | 配置≥32GB高速缓存，可扩展 |
| 二级缓存 | 可通过SSD固态硬盘和PCI-E闪存卡加速卡来扩展二级可读写缓存，二级缓存最大可扩展到≥1TB，从而提高存储的整体性能 |
| SAN加速功能 | 可通过SSD缓存加速功能监控磁盘的访问模式，然后自动将频繁访问的数据拷贝到固态硬盘组成的缓存中以加快读取速度，从而加速随机访问及整体I/O的读取速度，提供热点数据资源策略和访问统计信息的功能相关证明材料 |
| 前端主机端口 | 配置≥2个1Gb iSCSI主机接口，支持链路聚合和故障切换最大可支持12个GE网络接口模块，支持8/16GB光纤主机通道 |
| 容量配置 | 配置8个RD 4TB 7.2Krpm NLSAS硬盘和容量许可 |
| 灾备软件许可 | 提供核心业务和数据库的微秒级CDP保护许可 |
| 操作系统支持 | 支持基于X86平台Windows、Linux系统和国产操作系统、支持基于飞腾CPU平台的自主平台银河麒麟操作系统 |
| 服务器操作系统保护 | 通过ISCSI数据块协议（非TCP/IP网络协议），对服务器操作系统进行实时保护。当操作系统出现故障服务器可直接可通过SAN-BOOT方式远程启动操作系统；或直接通过金属裸机SAN-BOOT恢复 |
| NAS功能 | 该一体化保护设备要求提供NAS(NFS、CIFS)功能，提供NAS功能相关证明材料 |
| 压缩重删 | 支持数据压缩和重复数据删除功能，无需选择或者额外购买 |
| 自动精简技术 | 具有超额预定分配功能，能实现高效利用存储空间，减少已分配但是未使用的存储空间(需在产品配置清单中体现) |
| 虚拟机保护 | 提供对单个虚拟机系统和应用进行保护，可通过V2V和V2P(支持不同的硬件环境，无需转换)一键式恢复应用(需在产品配置清单中体现) |
| 物理机保护 | 提供物理服务器操作系统镜像和快照，可实现远程启动应用等功能或通过P2V和P2P(支持不同的硬件环境，无需转换)一键式恢复应用(需在产品配置清单中体现) |
| 自动化灾难恢复 | 在X86服务器损坏和应用不可用时，可支持通过灾备设备的一键恢复功能快速接管应用，实现自动化的灾难恢复。支持P2P,P2V,V2V,V2P(支持不同的硬件环境，无需转换)等方式的自动化故障切换和故障恢复 |
| 快照及代理 | 当前配置无限个数的应用软件感知型快照许可，单卷快照≥1000个，当前配置3套Snapshot Agent for MSSQL、3套Snapshot Agent for Oracle、3套Snapshot Agent for Domino数据库快照代理，保证数据一致性，快照立即可用无须恢复操作，服务器可以直接对快照进行读写操作。同时支持MSSQL、Sybase、Oralce、DB2、Domino、Exchange等数据库，支持基于X86平台的Windows、AIX、HP-UX、Solaris、Linux和基于飞腾CPU平台下国产自主银河麒麟等系统。在技术方案中阐述其基本的实现原理与客户实际应用不符合视为不响应标书要求(需在产品配置清单中体现)；提供数据库快照代理实现、快照挂栽等功能相关说明或证明材料 |
| 数据可用性 | 支持随时在不停业务系统和不中断容灾保护的状态下，挂载容灾存储的数据,验证数据是否可用，确保所有挂载数据正确可用 |
| 存储镜像 | 配置存储镜像功能，本地存储失效后直接切换到镜像存储，数据立即可用，保障生产应用不中断，数据”零”丢失(需在产品配置清单中体现) |
| ▲持续CDP保护 | 配置CDP持续数据保护和数据回滚功能，可以恢复最近一段时间内任意时间点(微秒级/百万分之一秒)的数据，可以准确定位到每一微秒的时间点的状态数据，采用非连续快照技术，提供微秒级持续数据保护功能的证明材料 |
| 本机数据恢复 | 当数据出现故障或不可用时，只需通过应用服务器的本机操作来挂接1个或多个历史快照来直接接管故障的数据盘对外提供服务，无需通过灾备保护系统的控制台进行操作，以及长时间的数据恢复和回滚。也可以通过灾备保护系统直接接管故障的数据盘对外提供服务 |
| 颗粒度还原 | 支持虚拟机颗粒度还原，无需在虚拟机上安装任何代理，同样的一体化备份，在还原时，可以选择想还原的具体指定文件、数据库、邮件、域控账号等内容，提供数据库颗粒度恢复的功能相关证明材料 |
| 自动验证 | 支持虚拟机备份后的自动恢复验证，确保备份的内容可恢复，并可以通过邮件告知管理人员自动验证的结果成功与否 |
| 虚拟实验室 | 支持应用沙箱试验，可在相对隔离的环境中运行备份虚拟机用于测试、开发、查询和故障排查等功能 |
| 虚拟机复制 | 支持本地虚拟机的复制功能，可以将虚拟机在灾备机上完整复制一份，当出现生产主机故障时，直接可以切换到灾备机上运行虚拟机，RTO<2分钟，同时支持远程广域网的虚拟机复制功能，提供虚拟机复制任务创建的功能相关证明材料 |
| 远程复制 | 支持IP网络或FC协议的压缩与加密复制，支持容灾系统级别一对一、一对多与多对多的同步/异步/增量双向复制，提供断点续传功能，具备窄带(非光纤)传输能力（容灾）功能，远程传输的数据块可设为不大于 512b字节（提供512b字节数据块复制功能相关证明材料） |
| SRM整合 | 灾备系统远程数据复制技术必须与VMware SRM(Site Recovery Manager)兼容,可接受VMware SRM(Site Recovery Manager)的调度管理，提供SRM相关插件 |
| 卷共享功能 | 提供六个节点的ImageSAN或StorNext卷共享软件（提供光盘介质及最终用户的许可证书），结构式共享SAN存储系统，任何一个节点的死机或重起，都不会影响用户对数据的调用。要明确说明本项功能实现的技术原理与客户实际应用不符合视为不响应标书要求(需在产品配置清单中体现)，提供Windows、Linux跨平台环境下卷共享的功能相关证明材料 |
| RDX归档 | 支持内置RDX自动归档功能，可内置具有热插拔功能的RDX磁盘，通过容灾系统的自动归档功能，把数据归档到RDX磁盘上，并保存多个历史时间副本，可实现数据的离线归档、长期保存，同时提供RDX硬件压缩功能和RDX加密功能，要求提供RDX归档功能的相关证明材料 |
| 硬件可靠性 | 完全的硬件冗余：处理器、缓存、电源、风扇、适配卡、总线等都提供冗余，并保证在某硬件出问题时，能够进行自动切换，不出现单点故障 |
| 在线告警 | 支持灾备保护系统的邮件、微信、短信等方式在线告警，实现硬盘、阵列、逻辑卷、CDP资源、快照资源、复制资源、镜像功能、SAN资源等项目的监控和在线通知功能，有任何故障可自动在第一时间通知生产厂商的售后支持中心获得支持 |
| 演练要求 | 在设备质保期内，厂商须免费提供每年一次的容灾演练服务承诺，相关要求由用户单位提出，需要在服务承诺函中体现 |
| 风险控制 | 一体化保护设备不能更改原有的服务器或存储映射关系，无需进行数据迁移，应用系统和保护设备的任何故障都互不影响，也不会影响到其他应用系统 |
| 产品证书 | 提供ISO9001，ISO14001，ISO27001，CCC，节能认证证书，并提供CDP软件著作权证书。 |
| 质量保证 | 为确保投标产品性能及功能真实可靠，对于技术偏离报表中功能性指标的响应需提供证明材料(提供相关证明材) |
| 服务保证 | 所投产品有成熟的服务支撑体系，派驻3名以上的技术工程师，常驻浙江省内工程师需提供最近3个月的浙江省内社保证明扫描件 |

**（10）堡垒主机（1台）**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 资质要求 | 产品资质 | 产品具有公安部颁发的计算机信息系统安全专用产品销售许可证、产品具有中国信息安全认证中心颁发的信息安全产品认证证书、产品具有国家版权局颁发的计算机软件著作权登记证书、通过国家保密局涉密信息系统产品认证 |
| 配置要求 | 产品架构 | 软硬件一体化产品 |
| 部署方式 | 采用物理旁路的方式接入，对现有主机和网络环境不做任何修改; 支持HA双机热备 |
| 支持分布式部署，智能负载均衡（提供相关说明或证明材料） |
| 管理结构 | B/S架构，采用HTTPS方式远程安全管理，无需安装管理客户端 |
| 系统支持 | 支持Windows、Linux、MacOS多种操作系统登录堡垒机运维设备主机 |
| 接口配置 | ≥100/1000M RJ45\*4个自适应以太网口 |
| 网络配置 | 支持网口聚合功能，防止单网口故障 |
| 数据存储 | 系统自带内部存储，物理磁盘空间≥4T |
| 可管理设备数量 | 本次配置200个设备许可证；最大可扩展到1000个设备许可证 |
| 安全系统 | 系统采用自制安全加固系统，精简内核、关闭了非必要功能，并对服务端口进行安全加固 |
| 性能要求 | 并发会话数 | 字符型协议（Telnet、SSH、FTP、SFTP）支持≥600个并发图形化协议（RDP、VNC及其他应用发布协议）支持≥100个并发 |
| 功能要求 | 目标资源访问 | 支持IE（8-11版本）、Chrome、Firefox、Safari通过 Web方式访问目标资源；Web访问方式支持屏幕分辨率、颜色深度、console开关等访问参数记忆功能 |
| 支持Telnet、SSH协议使用常用的客户端工具通过菜单选择方式或直接输入IP方式登录目标资源 |
| 支持协议 | 1.图形化协议：RDP、VNC、X112.字符型协议：Telnet、SSH(V1、V2)3.文件型协议：FTP、SFTP4.数据库协议：Oracle、Mysql、DB2、SQLServer、Informix、Postgresql、Sybase |
| 应用发布 | 支持通过应用发布的方式无缝发布应用给予本地化运维体验并对特定的客户端程序进行审计，支持VNCViewer、Xwin、ToadOracle、Radmin、SQLyog、PLSQL Developer、MSSQL Server、MySQL Front、Web、PostgreAdmin、VMware Vsphere、Network and Security Manager、easyview、cspsclient应用单点登录，支持定制开发单点登录应用，支持带参数应用发布 |
| 角色划分 | 系统角色需按法案要求进行划分，至少有系统管理员、密码管理员、审计管理员、团队主管、运维人员等多种角色；各角色功能定位明晰，不可越权 |
| 可根据业务需求创建自定义角色，自定义角色可在权限树上设置操作权限，权限树细化系统权限至按钮级别 |
| 支持角色以EXCEL方式批量导入、导出功能 |
| 身份认证 | 支持多种认证方式：本地口令认证、Radius认证、Radius二次认证、LDAP认证、AD域认证、内置动态口令牌认证、短信认证、手机动态口令认证、数字证书认证、双因素认证、混合认证 |
| 支持堡垒机原厂商动态口令牌认证，保证采购设备维护的一致性及兼容性;支持动态口令牌认证采用SM3国密算法且内置于堡垒机系统中，用户无需额外部署认证服务器  |
| 支持混合认证，可提供本地口令与动态口令牌、LDAP认证、AD域认证、Radius认证组合的双因素认证，以及动态口令牌与LDAP认证、AD域认证组合的双因素认证 |
| 登录堡垒机时可自动识别不同人员的登录认证方式 |
| 用户管理 | 支持用户帐号的整个生命周期管理，可方便添加、删除、修改、激活、未激活、注销、锁定用户账号；支持自助修改用户账号信息，包括密码、手机、邮件等基础信息；支持用户账号可设置部门属性，通过部门分级实现分权管理；支持用户账号以EXCEL方式批量导入、导出功能 |
| 支持批量修改用户帐号的属性，包括认证方式、角色、用户到期时间、IP登录规则、状态等信息；支持批量删除用户账号 |
| 可以根据需要，为外来人员分配临时用户帐号，该帐号拥有时效性，过期自动回收 |
| 支持用户账号密码强度管理，包括设定密码长度、密码复杂度、是否包含大写字母、是否包含小写字母、是否包含数字、是否包含特殊字符 |
| 支持用户账号密码使用期限设定，到期前一天邮件提示改密，到期后需改密后才可登录系统 |
| 支持在人员管理页面快速查看该人员可管理的设备 |
| 支持通过配置访问地址策略达到限制用户帐号只能在规定的地址段内进行资源访问；支持通过配置到期时间策略达到限制用户帐号只能在规定的时间内进行资源访问；支持通过配置访问锁定策略达到限制用户帐号密码输入错误次数 |
| 支持审批代理人设置并通过配置访问时间策略达到限制代理人只能在规定的时间段内进行代理审批 |
| 部门管理 | 支持部门分级管理，级别至少在三级以上；通过部门分级，实现对各类角色进行分权管理，使得不同部门的管理员、普通用户只能管理或者访问自己部门的资源 |
| 支持每个级别部门可分配部门领导功能；部门领导仅可查看本部门以及下属部门人员信息，禁止越权查看 |
| 支持部门的整个生命周期管理，可方便添加、删除、修改部门信息及部门成员；支持部门和部门所属设备以EXCEL方式批量导入、导出功能；支持批量删除部门信息 |
| 支持在部门管理页面快速查看该部门可管理的设备以及该部门所包含的人员 |
| 主机管理 | 支持主机设备的整个生命周期管理，可添加、删除、修改主机设备内容；主机设备可设置部门属性，通过部门分级实现主机设备只能本部门管理员管理 |
| 支持主机设备分组管理，可对设备组进行添加、删除、修改等操作；支持主机设备组以EXCEL方式批量导入、导出功能；支持主机设备组批量删除；支持按设备组快速授权用户 |
| 支持主机设备中幽灵账户手动收集、定时自动收集功能 |
| 支持主机存放地点组设置，可方便添加、删除、修改主机存放地点信息及存放地点组内设备选择；可对存放地点组进行批量删除；支持存放地点组所属设备快速查看 |
| 支持主机设备以EXCEL方式批量导入、导出功能；支持主机设备IP是否可达测试；支持主机设备端口是否打开测试 |
| 支持批量修改主机设备的属性，包括设备的状态（激活、禁用）、设备类型、所属部门、存放地点等；支持批量删除主机设备 |
| 支持主机账号的整个生命周期管理，可添加、删除、修改、激活、未激活主机账号内容；支持主机设备账号密码验证测试 |
| 支持主机账号以EXCEL方式批量导入、导出功能，并支持主机账号导入后自动关联主机设备无需手动关联 |
| 支持在主机管理页面直接查看该设备关联的授权清单及其管理人员；支持在主机管理页面直接设置主机设备协议、账号的授权清单关联 |
| 支持SSH协议客户端软件的Session Clone及Send To All等复杂克隆功能的审计 |
| 支持主机设备通过设置跳转设备实现不同设备之间的自动跳转登录；支持同一台设备上普通帐号与超级账号之间的自动代填切换登录 |
| 支持主机设备自定义检验脚本、运维脚本、改密脚本以及自定义脚本测试，实现所有主机设备的运维及改密功能支持 |
| 权限控制 | 支持单点登录功能，用户无需知道主机设备帐号及密码即可认证登录，无需进行二次登录认证；支持手工登录功能，用户登录目标设备时需手工输入账号及密码；支持半自动代填登录功能，用户手动输入设备密码后，系统会在下次登录时实现自动化登录 |
| 支持主账号传透功能，用户可用主账号（用户账号）直接登录主机设备，无需设置从账号（主机账号） |
| 支持设备运维登录备注功能，用户登录设备之前需填写备注内容后才可进行运维设备 |
| 支持通过制定授权清单将用户或整个部门与设备或设备组进行关系匹配；同时在授权清单中可以定义授权协议、设备账号等；授权清单可以对密码会同进行开启关闭设置，开启后用户可对设备进行密码会同操作 |
| 支持通过制定申请清单使运维人员可对清单中设备自主申请运维；申请清单可对用户或整个部门与设备或设备组进行关系匹配；同时在申请清单中可以定义授权协议、设备账号等 |
| 支持结合时间和来源IP制定高级访问控制策略，策略类型包括允许访问和拒绝访问；时间访问控制策略支持设置登录时间段方式（如每周一12：00-13：00，可循环），地址访问控制策略支持设置多个IP段方式，以确保可信用户访问其拥有权限的主机设备 |
| 支持高级访问控制策略可配置多条，每条策略可与授权清单进行关系匹配 |
| 支持配置命令黑白名单限制设备账号访问设备时，只能使用某些命令或者禁用某些命令；支持黑白名单命令匹配方式包括：模糊匹配、精确匹配、任意匹配，命令可匹配到参数；命令可设置风险等级 |
| 支持配置黑白名单时使用常用命令列表，方便用户指定黑白名单 |
| 支持对违规操作的指令（黑名单）进行单个命令的阻断、整个会话的阻断以及单独告警三种方式的设置 |
| 支持以邮件、页面、短信、syslog方式实时发送告警信息 |
| 支持黑白名单关联关系导入功能；支持用户或整个部门与设备或设备组授权关系一次性导入功能 |
| 支持图形协议的剪贴板、磁盘映射功能对不同人员、不同账号可单独设置开启/关闭功能；支持图形协议的console功能开启/关闭功能；支持调节图形协议的屏幕分辨率和颜色深度 |
| 操作审计 | 针对SSH、Telnet、FTP/SFTP、数据库操作进行记录及审计；记录发生时间、目标设备IP、客户端IP、操作命令、返回信息、服务器端口、协议、运维人员帐号、运维人员真实姓名、审批主管帐号、审批主管姓名、设备账号等信息；支持Word、Pdf方式导出 |
| 支持对字符协议的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出，可以展现各命令的执行时间点以及整个会话的访问时长、访问流量、命令数、告警和阻断数、合规违规状态等 |
| 针对RDP、VNC等图形终端操作的连接情况进行记录及审计；记录发生时间、发生地址、服务端IP、操作指令、返回信息、设备端口、协议、运维人员帐号、运维人员真实姓名、审批主管帐号、审批主管真实姓名、设备账号等信息；支持Word、Pdf方式导出 |
| 支持对图形协议的访问可以以录像形式审计到操作过程；支持操作过程的录像回放，可以展现键盘、鼠标、剪贴板操作的执行时间点以及整个会话的访问时长、访问流量等 |
| 支持对图形操作过程中的键盘鼠标操作、剪贴板操作进行文本审计并可对审计内容进行定位播放；支持Word、Pdf方式导出 |
| 支持图形协议操作过程缩略图预览并可对缩略图定点回放 |
| 支持输入输出在同一界面展示，并能以不同颜色自动标记出命令阻断、会话阻断、告警操作三种不同处理方式 |
| 支持以键盘输入内容、剪贴板的内容为关键字进行图形搜索；搜索出来的结果可以直接定位到相关图形画面进行回放 |
| 提供查询界面，供用户通过命令输入或命令输出的关键字、时间、客户端IP、目标设备IP、操作人、端口、账号名、协议条件进行组合查询 |
| 提供运维日志批注功能，供审计管理员查看并能够对所有会话进行合规性批注 |
| 禁止操作过程中通过敲击加\字符的方式绕过禁用限制 |
| 支持对所选协议批量运维以及操作过程的全审计 |
| 支持对会话进行实时同步监控，审计员可通过web管理界面实时监控运维人员进行的操作，并可手工中断危险操作会话 |
| 会话回放 | 支持以视频回放方式重现运维人员对设备的所有操作过程；支持倍速/低速播放、拖动、暂停、停止、重新播放等播放控制操作；支持空闲时间过滤 |
| 支持操作行为全文回放并且支持从任一条命令点处开始回放；支持回放录像中显示键盘输入、特殊按键、鼠标操作；支持下载视频文件到本地保存，并通过厂商专用播放器查看，防止会话视频记录泄密 |
| 密码管理 | 支持对Windows、Linux、Unix、Cisco、华为、H3C、锐捷、迈普等设备账号手动改密、批量自动改密功能 |
| 支持设备账号改密任务管理，可通过设置执行时间、执行周期、密码长度、密码策略等生成详细的改密计划到期自动执行，也可对改密任务进行立即执行操作 |
| 支持设置改密任务前多少天发送改密前邮件通知；改密前邮件通知以加密的方式发送改密确认链接、下次改密密码等信息 |
| 支持一键恢复设备初始密码功能 |
| 支持改密结果以加密方式自动发送至密码管理员邮箱或者FTP服务器；支持手动下载改密结果，改密结果以加密方式呈现；支持手动选择下载全部或者部分主机设备密码功能；支持改密结果以密码信封方式打印 |
| 支持改密方式包括随机生成不同密码、按组自动设置相同密码；自动设置的密码严格遵守密码强度设置；支持改密结果与前10次密码设置不同 |
| 支持改密任务下次执行时间提醒；支持改密任务以EXCEL方式批量导入、导出功能 |
| 支持改密日志记录，包括改密账号总数、成功数量、失败数量等信息，可方便查看改密结果；支持改密任务的统计报表，包括累计改密账号数、执行次数、成功次数等信息 |
| 脚本批量执行 | 管理员可以根据设备、系统账号、时间、脚本目录、脚本内容、结果存放目录等创建自动脚本任务；该任务到期自动执行，执行的结果自动发送给相关管理员或者保存到FTP服务器 |
| 支持脚本上传后需通过上级主管审批后才可执行；若有多级主管，可自定义中间人审批权限为审批通过、审批拟通过、审批拒绝、审批拟拒绝多种审批权限 |
| 网络设备配置备份 | 可以通过内置的脚本，定期自动备份指定的网络设备上的配置，备份结果自动发送给相关管理员 |
| 特殊运维 | 运维人员能够自行发起主动运维申请，提交自己需要运维的主机及本次运维需要执行的命令；部门领导审批通过后，运维人员才可按照申请内容进行运维，否则无法进行任何操作 |
| 支持多级主管审批，一级主管可将运维申请上交给分管领导做二次审批 |
| 支持多级审批中间人自定义审批权限，可自定义中间人审批权限为审批通过、审批拟通过、审批拒绝、审批拟拒绝 |
| 支持领导通过页面和邮件方式进行运维申请审批；支持审计员对运维申请进行作废处理 |
| 支持多种运维模式包含：系统变更、需求处理、巡检、硬件维护、应急演练、故障处理、紧急故障处理等多种运维场景 |
| 提供领导离线审批功能，仅需匹配领导的登录账号和动态口令牌口令即可自动通过审批；支持短信提醒领导有特殊运维申请待批复信息 |
| 双人协作 | 对于重要设备的危险指令操作，需要有复核人对运维人员的操作进行复核后才可继续操作 |
| 对于图形操作会话支持多人会话共享，当前运维人员可以邀请其他用户共享或者协助当前操作会话 |
| 支持双人通过输入前段密码或后段密码方式进行密码会同，通过后才可进行设备运维 |
| 审计报表 | 支持统计出某段时间内，审计管理员自定义的重点命令以及重点命令集执行情况的报表，包括各个用户操作重点命令的次数、重点命令的会话次数、重点命令的执行会话；支持重点命令会话回显以及定位播放 |
| 支持预设常用统计报表模板，包括以部门和人员为主要对象，统计其工作量的报表；以账号登陆为统计对象的报表；以黑白命令为统计对象，统计敏感命令使用情况的报表；以设备和人员为统计对象，记录其日常工作的流水报表；以日、周、月、季度、年为周期做统计的报表；对运维次数、运维Top10、主机访问量做统计的报表；对堡垒机管理人员的管理操作做统计的报表；根据等级保护的标准对设备运维进行全面统计的报表 |
| 支持对特殊运维申请的主机数、账号数、命令数等条件和特殊运维审批中一级通过数、二级通过数等条件以及双人协作中运维数等条件进行统计展示 |
| 支持按照预设统计报表模板，根据时间、人员、部门、设备、运维类型、设备账号、设备地址、设备端口、命令关键字等条件形成统计报表，统计报表支持Excel、Word、Pdf格式导出 |
| 支持按照以日、周、月设置报表邮件发送执行时间并可根据时间、人员、部门、设备、运维类型、设备账号、设备地址、设备端口、命令关键字等形成筛选条件根据筛选条件发送报表内容 |
| 系统管理 | 支持实时监控堡垒机CPU、内存、磁盘的使用情况；支持堡垒机主题换肤功能，可切换深色和浅色两种主题版本；支持中文、英文操作界面；支持所有弹出框可进行拖动 |
| 支持对堡垒机中配置信息、日志信息和运维信息进行选择性定期归档；支持系统登录日志、操作管理日志、导入导出日志查看；支持以FTP、SFTP方式自动上传归档信息；支持归档信息导入并恢复； |
| 支持磁盘空间预警功能，可按照磁盘百分比和大小设置告警阈值，触发告警时可通过邮件、短信、Syslog发送告警通知；支持空间自管理功能，存储空间不足时能够设置转存空间大小和转存地址并自动清理旧数据 |
| 支持SNMP协议配置获取系统信息; 支持Web服务器证书页面下载 |
| 支持页面无操作超时自定义时间设置；支持双人协作无复核超时自定义时间设置；支持文本协议、图形协议、文件协议、数据库协议使用的多种客户端全局化设置，保证运维人员快速使用常用工具，无需选择多种客户端；支持设置运维页面信息列的选择性显示和隐藏，防止敏感信息泄露，并可对信息进行升序或降序排列 |
| 支持WEB界面修改网卡IP设置、静态路由设置等功能；支持WEB界面时间同步设置功能；支持WEB界面重启、关闭堡垒机设备功能；支持WEB界面进行系统升级功能；支持查看所有在线运维人员 |
| 为保证项目的顺利实施与信息安全保障能力，须具备中国信息安全认证中心颁发的《信息系统安全集成服务资质证书》、《信息安全风险评估服务资质证书》，通过ISO27001信息安全管理体系认证 |

**（11）网络安全信息集成要求**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| ▲基本要求 | 对原有的网络安全设备进行优化调整。依据国家标准GB/T22239-2008《信息安全技术信息系统安全等级保护基本要求》且满足以下需求：要求按照等级保护规定将网络按照安全域划分，按照双网隔离方案分为信息内网和信息外网。安全域实现方式以划分逻辑区域为主，旨在实现各安全区域的逻辑划分，明确边界以对各安全域分别防护，并且进行域间边界控制。进行等保测评时，现场配合测评，并按要求免费提供技术现场支持。 |
| 安全域的划分 | 防火墙安全隔离：采用防火墙 进行边界隔离，在每两个安全域的边界部署防火墙分别与不通的安全域连接进行访问控制，防火墙采取三权分立原则；虚拟防火墙隔离：采用虚拟防火墙实现各安全域边界隔离，将一台防火墙在逻辑上划分为多台虚拟的防火墙，每个虚拟防火墙系统都可以被看成一台完全独立的防火墙设备，可以拥有独立的系统资源、安全策略等； |
| 要求定期对网络环境，网络设备，系统进行检测，有问题或者漏洞补丁更新做到及时处理： |
| 针对网络设备： | 启用访问控制功能，依据安全策略控制用户对资源的访问；关闭防火墙设备、交换机的telnet服务，启用安全的SSH和https管理服务；修改网络设备出厂时的默认口令，且口令应满足长度不小于8为、含字母数字和字符的复杂强度要求；网络设备，防火墙交换机等要求开启日志审计功能，并配置日志服务器保存日志信息；要求调整现有审计设备，审计范围覆盖到服务器和重要客户端的每个操作系统用户；要求审计内容包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内的重要相关时间；要求审计记录包含事件的日期、时间、类型、主体标识、客体标识和结果等；所有网络设备均应开启网络设备登录失败处理功能、限制非法登录次数、当网络登录连接超时时自动退出等措施； |
| 针对操作系统 | 结合我单位现有网络设备或系统；要求实现操作系统特权用户的权限分离，即三权分立；要求限制默认账户的访问权限，重命名系统默认账户，修改账户的默认口令；要求及时删除多余的、过期的账户、避免共享账户的存在；要求对主机的登录要有严格的身份标识和鉴别；要求有严格的访问控制策略限制用户对主机的访问与操作；要求有严密的安全审计策略保证主机出现故障时可查； |
| 信息安全风险评估 | 分析机房所有信息资产（包括硬件、软件、文档和数据、人力、业务应用、物理环境、组织管理等）的稳定性、可靠性、保密性、可用性、完整性等安全属性，对涉及安全的关键资产进行确认和划控。 |
| 对资产（包括硬件、业务应用、物理环境、组织管理等）面临哪些潜在威胁，导致威胁的问题所在，威胁发生的可能性有多大等问题进行分析。 |
| 从技术方面，全面分析系统存在的各种脆弱性，分析弱点被利用的可能性。 |
| 分析已有的安全措施对安全风险的控制作用； |
| 分析当前系统仍存在的风险并给出相应控制和管理风险的建议； |
| 提供评估报告； |
| 信息系统加固修复 | 对现有信息安全管理体系中存在的问题进行优化和完善，并协助甲方完成相关文档的编写和宣传 |
| 对全网的网络设备和安全设备进行修复加固和漏洞扫描 |
| 确认主机操作系统、应用系统的安全策略未被更改或还原 |
| 查找现有信息安全管理制度与三级要求之间的差距 |

**2．数据安全防护系统要求**

**（1）加密服务平台（1套）**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| ▲产品合规性要求 | 方案中服务器密码机属于密码专用设备，集成的产品需要具有国家密码管理局颁发的商业密码产品型号证书。 |
| 数据加解密功能 | 提供数据加解密以及密钥安全管理功能，确保数据加密算法及密钥的安全性，为应用安全防护与数据安全防护提供安全服务与加密服务。 |
| 密码算法要求 | 支持国家商用密码规定的密码算法，包括SM1、SM2、SM3、SM4算法。 |
| 密码应用接口要求 | 提供 数字签名/验证签名/会话密钥协商/数字信封、消息杂凑、消息验证码MAC产生/验证、物理噪声源生成真随机数等服务器密码机功能 |
| 集群化部署 | 提供集群化的架构设计解决方案，有效防止单点故障，提供7\*24的安全服务能力。 |
| 兼容性需求 | 平台兼容本期项目中所有受保护目标应用系统的运行环境。 |
| 统一管理功能 | 提供统一的可视化管理界面，易于后期维护管理和系统升级扩展。 |

**（2）数据库安全防护平台（1套）**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| ▲产品合规性要求 | 集成的信息安全产品需要提供中华人民共和国公安部颁发信息安全专用产品销售许可证。 |
| 数据库攻击防护功能 | 提供[数据库](http://baike.baidu.com/view/1088.htm)攻击防护功能，能够对常见的数据库攻击，包括[口令入侵](http://baike.baidu.com/view/987197.htm)、特权提升、SQL注入等攻击进行检测并阻断。 |
| 数据库加强访问控制功能 | 提供安全访问控制功能，能够限制对象（数据库用户）、限制访问数据库的地址；限制用户对数据库的各种操作等。 |
| 数据库访问权限限制功能 | 提供数据库访问权限限制功能，能够针对数据库对象（库、表等）进行访问权限设置，防止越权读取修改数据。产品若支持元数据主动防御功能，如采取混淆或加密等方式防止外部逆向分析，优先考虑。 |
| 数据库管理工具安全防护 | 产品能够限制操作数据库的客户端工具（数据库管理工具）和应用程序列表，防止数据库的非法接入与越权操作。 |
| 数据库审计功能 | 对数据库操作进行审计，至少审计内容包括事件主体（IP地址、MAC地址）；事件客体（被访问对象库、表等）；访问时间；访问类型（对数据库的各种操作）；访问结果（数据库返回的结果）。 |
| 数据库主动防护功能 | 对业务应用程序中数据库操作代码混淆编码变换，有效防止各类代码注入攻击方式（如SQL注入攻击等）。支持SQL命令关键字动态编码变换，对针对数据库的SQL注入攻击提供完备的防御机制。**功能需提供相关证明材料**。 |
| 信息动态编码防护 | 支持对数据库管理工具查看信息的动态编码保护功能，信息在使用中采用非明文使用和传输，防止数据泄露风险。**功能需提供相关证明材料**。 |
| 防护库升级功能 | 提供数据库漏洞库、数据库功能特征库的升级能力。 |
| 集群化部署 | 提供集群化的架构设计解决方案，有效防止单点故障，提供7\*24的安全服务能力。 |
| 兼容性需求 | 平台兼容本期项目中所有受保护目标应用系统的运行环境。 |

**（3）应用安全防护平台（1套）**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| ▲产品合规性要求 | 集成的信息安全产品需要提供中华人民共和国公安部颁发信息安全专用产品销售许可证。 |
| 产品合规性要求 | 通过网络关键设备和网络安全专用产品安全认证和安全检测，整机应用整机应用吞吐量≥6Gbps、最大HTTP并发连接数≥200万。 |
| WEB应用安全防护 | 支持WEB应用安全防护，有效识别并拦截利用WEB服务器漏洞以及主流脚本语言漏洞进行的攻击。产品能提供SQL注入防护、XSS攻击防护、盗链防护、CSRF防护、Cookie注入、Webshell识别拦截、爬虫防护、非法上传下载等安全功能。产品支持对HTTP过滤功能，提供对HTTP请求、字长、响应码以及关键字等信息进行限制过滤的功能。 |
| HTTP过滤功能 | 支持HTTP请求类型过滤功能、支持HTTP 协议头各个字段的长度限制功能、支持文件后缀名过滤功能、支持识别和限制 HTTP 响应码功能、支持URL内容关键字过滤功能、WEB 服务器返回内容过滤功能。 |
| 信息安全主动防御机制 | 支持系统前端页面字符、资源标识（URL）、网页代码（POST请求参数）的动态变换，有效防止针对网站的逆向分析；防止BOT、网络爬虫等攻击；防止网站内容被非法拷贝或者爬取。**提供计算机信息安全专用产品的检验检测报告**。 |
| 支持白名单功能 | 根据白名单规则（IP等），对HTTP访问请求进行阻断 |
| 支持HTTPS功能 | 可对HTTPS协议进行解码，并依据过滤规则允许或阻断该访问请求 |
| 支持安全规则管理功能 | 可依据默认的安全防护规则库进行防护；对安全防护规则库进行升级；添加 、删除、修改自定义过滤规则可生效，并依据该自定义过滤规则允许或阻断该访问请求。 |
| 支持应用安全审计功能 | 提供安全日志审计功能，审计日志内容是否包括每个事件发生的日期 、时间、IP 地址 、所请求的 URL 、访问成功或失败的标识以及匹配规则等。 |
| 集群化部署 | 提供集群化的架构设计解决方案，有效防止单点故障，提供7\*24的安全服务能力。 |
| 兼容性需求 | 平台兼容本期项目中所有受保护目标应用系统的运行环境。 |

3**．安全服务的技术要求**

**（1）总体概述要求**

|  |  |
| --- | --- |
| 服务内容 | 服务简述内容 |
| 安全监控 | 1. 持续关注客户网络、系统运行情况，一旦发生安全事件后，及时分析安全系统及设备的事件日志，配合甲方进行事件的追踪定位。
2. 通过对项目范围内所有安全系统及设备的报警日志进行分析客户近一月的信息安全情势、安全状况，提出改进建议。
 |
| 安全预警 | 1、服务期内以报告形式向甲方公布常规漏洞通报，内容包括国内外权威漏洞发布公开站点为主要数据源的安全漏洞信息（如CVE、NVD、Bugtraq、CERT等）；2、遇重大安全漏洞或事件时，实时向甲方通报事件预警，提供防护或规避建议；3、及时了解本省网络安全监管单位最新动向，对已知安全风险问题处置风险，避免被通报及法律法规责任。 |
| 安全设备管理 | 1、对项目范围内的所有在运行安全系统及设备进行巡检，对设备的物理运行情况、清洁情况、系统运行情况、系统资源利用情况、系统运行日志、相应功能是否正常运行等进行检查并记录，排除可能存在的安全问题和隐患。2、对设备配置、日志进行备份。3、在安全设备故障处理过程中的所有协调配合及总结报告工作。 |
| 安全策略管理 | 1. 根据安全运维工作需要，对安全设备自身的配置进行变更调整，如登录口令、登录方式、密码复杂度等设备运维策略。
2. 每月对安全设备业务访问策略进行梳理分析，发现过期、冗余、无效、不明确用途等策略，根据分析结果提供优化调整建议；
3. 配合业务系统部署与调整，从安全角度给出部署建议，制定和更新安全设备的防护、检测策略。
 |
| 安全事件管理 | 在发现或发生安全事件后配合相关汇报、跟踪、总结汇报、记录工作。 |
| 安全检查 | 1、通过安全扫描工具定期对客户信息系统进行漏洞扫描和配置检查；2、为本单位内部的相应迎检及对外检查工作提供技术支持3、为本单位内已经定级备案系统提供协助等级保护测评工作，并在测评前提供预测评工作，保证本年度顺利通过等级保护测评(涉及设备采购及业务系统代码层面问题由本单位自行协调) |
| 安全加固 | 1、定期对操作系统、网络设备进行加固2、定期加固操作系统、数据库、网络设备、应用系统、安全设备配置及策略优化3、重大活动或敏感时期，根据实际情况在安全运维范围内执行相应加固工作 |

**（2）驻场服务**

**服务要求**

提供一名驻场运维人员，负责信息系统日常安全维护技术服务，做好安全防护策略制定，运行日志审计，开展防病毒检查等日常工作。驻场人员需了解HUAWEI、H3C、天融信、启明星辰、DELL等主流网络、服务器、安全设备。

**实施周期**

服务期内工作日。

**（3）资产调查服务**

**服务要求**

经招标单位授权，对省委编办信息系统的关键资产进行识别，并合理分类；在资产识别过程中，需要详细识别核心关键资产的安全属性，重点识别出资产在遭受泄密、中断、损害等破坏时所遭受的影响，并据此对资产的价值进行赋值。

建立完善的托管物理设备设备档案，随时更新设备配置信息档案库。

**实施周期**

服务期内每月更新一次。

**（4）数据备份服务**

服务要求

经招标单位授权，对省委编办托管外网服务器数据进行备份，如发生突发状况，做好数据恢复工作。以三个月为周期，对所备份的数据进行磁带刻录，并对备份数据进行恢复性测试，并按时于每个周期结束后5个工作日内，将磁带交予甲方。

**实施周期**

省委编办提供备份软件和备份磁带,每天增量备份、每周全备份、每月进行一次数据归档。

每三个月提供一次磁带。

**（5）运行监控服务**

**服务要求**

网络及设备的监控及巡检，及时发现并处理网络和设备故障，并定期备份设备配置。

对服务器系统监控，通过系统监控、进程监控、日志分析，及时排除安全漏洞，优化系统。

对应用系统监控，通过日常监控和安全通报及时发现故障或漏洞，提供程序安全改进建议。

持续关注客户网络、系统运行情况，一旦发生安全事件后，及时分析安全系统及设备的事件日志，配合甲方进行事件的追踪定位。

定期通过对项目范围内所有安全系统及设备的报警日志进行分析，梳理客户近一月的信息安全情势、安全状况，提出改进建议。

**实施周期**

服务期内每日。

**（6）服务器安全服务**

**服务要求**

经招标单位授权，每周对服务期设备进行维护，维护内容包括系统账户管理、权限管理、补丁更新，进程监控及系统故障分析。

日志分析：通过系统监控、运维日志、系统日志分析，调整系统配置参数，进行系统平台优化。

通过安全扫描工具定期对省委编办信息系统进行漏洞扫描和配置检查；

**安全配置检查：定期使用安全配置核查工具对操作系统、中间件、数据库、网络设备的配置进行检查；涉及的工具软件须具备公安部销售许可证。**

**漏洞扫描：定期使用漏洞扫描工具对应用、主机进行漏洞扫描，根据扫描结果做出安装补丁、关闭端口等调整操作；要求本次使用的系统脆弱性扫描工具具备公安部销售许可证。**

**实施周期**

服务期内每周。

**（7）网络安全防范及处置**

**服务要求**

经招标单位授权，在各安全设备上设置事件告警，告警方式根据设备支持情况可以是短信、邮件、日志等形式；如进行告警配置需要进行安全设备策略修改的，根据实际业务需求对安全设备进行相关策略修改、优化。调整入侵检测设备策略，实时阻断外部入侵行为，清除恶意代码攻击，防范SQL注入等，在发生严重入侵事件时提供报警。

对网络流量、用户访问行为等进行日志记录，定期进行审核。关注相关告警日志及当前网络实际运行状况。进行必要的告警日志分析。当客户网络实际运行水平出现明显下降，或明确发生安全事件时，及时配合进行相关设备的检查并提供程序安全改进建议。

**实施周期**

服务期内每周。

**（8）网络评估服务**

**服务要求**

经招标单位授权，通过业务调研、网络分析、人工检查等方法进行综合评估并每个业务系统形成独立的安全评估报告。安全风险级别采用科学的风险定级方式，针对相关影响及利用难易程度进行安全分析，保证安全评估结果有效。

**安全服务商评估人员须为具有过网络安全等级测评师中级以上及浙江省人力资源和社会保障厅专业技术资格，具备PDPF（隐私和数据保护认证）认证、MCP认证。**

**实施周期**

服务期内每年一次。

**（9）病毒查杀服务**

**服务要求**

经招标单位授权，对省委编办所有网络内的设备进行病毒查杀，对于防病毒软件无法处理的病毒，现场服务工程师将采用标准的病毒处理流程进行手工清除。

**实施周期**

不定期。

**（10）网站实时监控**

**服务要求**

对省委编办对外网站进行实时监控，对网站可用性进行监测、网页敏感内容监测、网站可用性监测、网页篡改监测。

**实施周期**

不定期。

**（11）等保评估辅助**

**服务要求**

基于国家信息安全等级保护相关标准和文件要求，结合省委编办信息系统的安全保护等级，对信息系统安全等级保护状况进行安全评估，对信息安全管控能力进行考察和评价，确定信息系统安全保护能力是否达到相应等级基本要求的过程，以帮助省委编办及时发现信息安全风险，明确安全需求，达到最终通过等保测评的目的。安全服务商评估人员须为具有过网络安全等级中级以上测评师。

**实施周期**

服务期内按需实施。

**（12）应急响应服务**

**服务要求**

重保期间提供7\*24小时的应急响应服务支持，半小时内响应，两小时做好数据恢复。应用系统故障时，配合软件开发单位做好应用系统恢复。

**实施周期**

服务期内6次。

**（13）安全服务商资质要求**

1、安全服务商项目经理（提供社保证明及劳动合同扫描件）：

**项目经理具有PMP证书、CCSK证书、CISP、ITIL证书、MCTP证书、RHCE证书，以上证书须提供复印件。**

2、安全服务商须为中国信息安全测评中心颁发的“国家信息安全测评信息安全服务资质证书（安全工程类三级）”，须提供上述证书复印件。

3、安全服务商须为网络安全应急服务支撑单位（国家级），须提供上述证书复印件。

**4、安全服务商为《GBT22239-2019信息安全技术网络安全等级保护基本要求》、《GBT25070-2019信息安全技术网络安全等级保护安全设计技术要求》、《GBT28448-2019信息安全技术网络安全等级保护测评要求》标准的起草单位，须提供证明文件。**

5、安全服务商须为中国网络安全审查技术与认证中心颁发的“信息安全风险评估资质（一级）”证书，须提供上述证书复印件。

6、安全服务商须为中国网络安全审查技术与认证中心颁发的“信息安全应急处理资质（一级）”证书，须提供上述证书复印件。

**7、安全服务商须为2020年度浙江省网络与信息安全信息通报中心技术支持合作单位，须提供证明。**

**8、中国国家信息安全漏洞库（CNNVD）技术支撑单位一级，须提供证明。**

**9、信息安全等级保护安全建设服务机构能力评估合格证书，须提供证明。**

4**．实施要求和服务培训**

**（1）实施要求**

对于本招标文件未列明，而投标人认为必需的费用也需列入投标报价。在合同实施时，采购人将不予支付投标人没有列入的项目费用，并认为此项目所需的费用均已包括在投标总报价中。对在合同实施过程中可能发生的其它费用（如：材料涨价、人工、运输成本增加等因素），采购人概不负责。

本项目需投标人完成项目产品提供、系统集成、安装、调试、报检、培训、售后服务等内容，费用需计入投标报价。

投标人在产品供货时，硬件产品必须是针对本用户的，设备外包装用户名必须为浙江省委编办，并提供产品序列号备查。

项目实施周期要求：按“一、采购内容一览表”中规定。

交货地点：用户指定地点

投标方应提供详细的项目实施方案，说明项目的实施计划、实施过程、流程、质量控制措施、成功保障措施、项目完成后交付的成果文档以及其它认为需要的说明的内容。

**（2）验收要求**

验收前，需符合等保相关要求，并通过测评，方可验收。

**商务要求表**

|  |  |
| --- | --- |
| **▲供货时间（项目工期）及地点** | 货物供货工期：合同签订后30天内安全服务时间：双方合同签订后12个月交货地点：用户指定地点 |
| **▲付款条件（明确是否需要履约保证金）** | 合同签订后十个工作日内，预付款项为合同额的20%；所有货物到货后支付合同额的43%；待项目终验后一次性付清合同总金额的余款。备注：1、本项目不需要履约保证金；2、本项目部分款项为跨年度支付。 |
| **违约责任及争议解决方式** | 如无特别说明，按“浙江省政府采购合同主要条款指引”相关违约责任及争议解决方式内容。 |
| **售****后****服****务** | **项目维护计划** | 质保期为三年，质保期从最终验收合格之日起计算。（其中安全服务期限是一年，以合同签订之日起计算）中标人应根据用户要求与实际情况负责完成本项目的所有系统集成相关的安装调试工作，解决实施过程中的全部技术问题；凡在本次项目实施时，如需对原有的系统架构进行相应的调整，中标人应根据用户的实际要求，提供相应的技术支持，由此所涉及的相关费用，由中标人负责。对于项目实施后出现的软硬件故障，中标人提供7\*24小时的技术支持并提供专门的项目技术小组，由于客户特殊性故障出现后立刻响应并在2小时内赶到客户现场。对于项目中的软硬件设备，中标人需要给业主单位提供定期的设备巡检服务，其中包括免费的软件系统升级和故障处理。 |
| **响应情况** | 妥善安排售后服务人员和驻场服务人员，确保提供7\*24小时服务响应服务，要求在12小时内响应采购人提出的疑问和修改意见。投标时标明常用备品备件及耗材的投标价，24小时故障无法修复免费提供备机。 |
| **技术培训** | 中标方免费为用户提供培训。包括：培训讲师和培训材料，培训时间不少于2天，培训人数不少于2人。在投标文件内提供针对性培训方案，应详细说明培训的内容、计划、方式、地点、人数、时间等实质性内容，并承担所有费用。 |
| **履约能力** | **公司技术力量情况** | 投标商具有信息系统集成及服务资质、国家涉密资质、国家高新企业等证书。 |
| **经验或业绩要求** | 自2017年1月1日以来省级类似成功项目业绩，提供合同复印件需加盖公章。（每提供一个得一份，最高3分） |

标项3:政务云安全服务项目

一、项目概述

根据省政府的统一要求，省委编办已完成如实名制系统、事业单位登记管理系统、数据仓等多个核心业务系统的迁云上云，更多业务也正逐步迁移至政务一朵云，其中部分系统存储有大量客户数据及敏感信息，部分系统与互联网有互联接口或本身为互联网一部分，云上业务面临着各种潜在的安全风险和威胁。

为确保各生产系统正常运行、满足省委省政府网络与信息安全责任考核以及各监管部门的各类安全考核要求，切实落实新上云资产的安全要求、加大各系统内部安全自查力度、满足云上安全规范、快速定位并及时处理云上各类信息安全问题、实现7\*24小时专业安全应急保障，提升维护及安全技术人员技能，需要引进专业安全厂家提供信息安全技术服务，提升省委编办云上整体安全运维管理能力和安全维护水平。

云上安全服务工作内容包括：安全运维工作（日常安全运维、日常安全巡检、安全策略加固、安全事件处理、周期性工作等），自动化安全监控工作（云资产自动化覆盖、Web漏洞监控、主机漏洞监控、组件漏洞监控、攻击面监控、修复指导、应急响应、钉钉及邮件告警、服务报告输出等）、其他安全工作（安全事件应急演练、云上安全培训等）。

**二、工作目标**

清楚了解省委编办所有云上业务系统的安全现状，发现面临的安全威胁和风险。包括云资源安全、网络架构安全、业务流程安全、应用安全、数据信息的安全存储与传输等。针对安全威胁和风险采取必要的措施进行安全加固、补丁升级、风险规避服务；提供专业、持续有效的安全运维、自动化监测服务及技术支持，提升省委编办云上整体安全运维管理能力和维护水平，确保各类安全风险在可管可控范围。

**三、服务范围**

**（一）远程技术支持服务**

▲提供至少3人的5\*8的专人远程业务支撑服务，完成计划内的云上安全运维、自动化安全监控等工作并定期以报告的形式报告工作情况。

根据各项工作的具体要求，定期提交工作报告，真实的反应信息安全现状及各项工作的进度，以降低信息安全风险，为下阶段工作的安排提供参考，不断推进信息安全技术及管理工作的完善。

**（二）高级技术支持服务**

提供安全专家技术支持服务，有丰富应急攻防演练及安全培训经验的工程师对省委编办云上业务进行1次应急演练及1次云上安全培训服务，帮助建立并完善应急响应机制，提高业务人员应急处置能力，合理规范、高效地应对突发安全事件及异常情况，并通过培训让业务及系统运维人员了解并掌握云上安全规范、安全机制与架构，以及各云产品的安全功能，便于提高云上安全运营能力。

**（三）紧急业务支持服务**

提供7\*24的紧急业务支持服务，当省委编办云上业务需要紧急安全服务支持时，或者有重大和棘手的安全情况发生时，为提高处理速度和处理质量，应增加“资深紧急人员”通过远程方式进行跟踪处理，如有需要应到现场处理。

**（四）项目工作实施范围**

本次安全服务项目将覆盖省委编办负责维护的所有政务一朵云上生产及测试系统，包含但不限于：

业务系统：实名制系统、事业单位登记管理系统、钉钉办公系统、数据交换平台、数据仓系统以及项目服务期内上云新业务。

云基础资源：VPC内所有云产品，如NAT、ECS、SLB、RDS、OSS、安全组、网络组件等。

安全设备与平台：阿里云云盾、主机防护软件、堡垒机、数据库审计、Web应用防火墙等。

**四、服务时间要求**

本项目服务期限：一年（签订合同日起计算）。

工作时间：与省委编办工作时间一致

日常远程支持：5\*8小时

紧急业务支持：7\*24小时

情况说明：维护时间的要求解释权在省委编办，省委编办根据实际业务情况的变化，可以对该时间进行调整。

**五、服务能力要求**

**（一）服务团队要求**

安全服务团队应保证100％的团队成员熟悉省委编办的相关安全管理规范和业务流程；日常安全服务人员应保证100％本地化，保障售后响应支持。

项目组人员至少3人，1名项目经理须具备信息系统多年相关管理经验，具备项目管理PMP认证证书和由人社部分颁发的信息系统项目管理师（高级）证书；2名项目成员熟悉阿里云产品，须具备阿里云ACP认证。

**（二）省委编办提出的维护人员更换**

省委编办根据远程服务人员工作态度、工作能力、出勤率和沟通能力等各方面工作情况，有权决定更换服务人员。应在省委编办提出更换人员要求的3天之内，安排其他符合要求的业务支撑人员提供服务。

**（三）服务厂商的要求**

1、遵守国家电子政务和信息产业部有关法律法规和技术标准，提供安全、客观、公正的安全运维及监控等服务，保证服务的质量和效果。

2、保证在安全运维及监控等安全服务活动中知悉的国家秘密、政务机关单位秘密、企业秘密和公民隐私，防范相关工作带来的风险。

3、对相关工作人员进行安全保密教育，与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。

**六、服务内容要求**

**（一）安全运维服务**

**概述：**对省委编办在政务一朵云上的所有业务系统、安全产品、云资源开展安全运维服务，包括但不限于：安全产品配置及优化、云资源及安全中心日常安全巡检、安全策略加固、安全事件排查溯源、安全运维周期性工作等。

**工作目标：**满足云上安全规范及最佳实践要求，全面保障云上资产安全性，增强安全运维能力，提供事前、事中、事后的全生命周期安全保障。

**工作内容及要求：**

日常安全运维：对云盾及安全产品进行日常安全运维配置，如产品接入、配置优化等。

日常安全巡检：日常对云上资产安全配置情况、各类安全产品进行巡检，如：ECS安全组、RDS白名单、云盾安全中心、主机防护软件、堡垒机、数据库审计、Web应用防火墙的安全状态等。（巡检频率：每天不少于两次）

安全策略加固：依据政务一朵云最佳实践，从虚机、网络、数据、Web应用等层面对云产品和安全产品进行有效的安全策略设计，充分保证云上应用和数据的安全。

安全事件处理：发现安全事件或攻击事件后，进行有效防护处理及溯源分析。

周期性工作：1）定期提供安全事件、攻击、漏洞报表，清晰展现系统安全状况及趋势；2）自动更新Windows、Linux操作系统补丁，防止黑客利用已知漏洞进行攻击；3）对云盾及其他安全产品的安全规则库进行更新，防御零日漏洞攻击。

**工作输出：**每月提交《xx月安全运维服务报告》

**（二）应急演练服务**

**概述：**协调省委编办及各系统业务方、运维人员开展安全事件应急演练及相关技术支持工作。

**工作目标：**提高省委编办各业务方应急人员在遇到安全事件及问题时的应急操作水平，最终实现应急人员、应急预案和应急操作的协调，提升省委编办的安全应急保障能力。

**工作内容及要求：**

协助编制应急演练预案

须根据省委编办安全管理相关要求，结合省委编办年度应急演练工作计划和招标方公司实际情况，设计安全突发事件的应急预案和处置方案。

协助应急演练

根据省委编办确定的演练范围和内容开展1次应急演练，并提供安全预演、场景搭建等服务。

重要时期应急支持服务

合同有效期内，根据特殊重要时期保障的需要，协助做好整体应急统筹安排，编写重要时期应急工作方案，开展应急值守保障工作。

**工作输出：**

《xx应急处置预案》

《xx应急演练实施方案》

《xx应急演练脚本》

**（三）安全监控服务**

**概述：**提供云上安全监控系统，与政务一朵云平台无缝结合，为省委编办提供云上资产自动发现、漏洞自动扫描、云平台安全配置检查、实时告警/报表等功能服务，及时发现安全漏洞及风险隐患，并提供安全事件应急响应及安全技术服务。

**工作目标：**实现云上资产自动化风险监控及实时告警能力，降低人力安全运营成本，提高风险管控及处置效率。

**▲工作内容及要求：（提供后台功能证明材料）**

云资产自动化覆盖：在获得省委编办授权许可后，自动识别省委编办在政务一朵云上的ECS、SLB、NAT IP、Web域名、安全组策略等资产，加入监控范围。

漏洞监控功能：具备自动化Web漏洞、主机漏洞及Apache、Tomcat、Jekins等应用组件、框架的漏洞发现能力。

攻击面监控：自动发现云上安全组、弱口令、IP白名单、非授权对外IP、高危端口、中间件等可能存在的危险攻击面。

修复指导：针对自动化监控服务发现的安全风险，通过电话或钉钉提供远程修复指导。

应急响应：当发现高中危安全事件或安全漏洞时，提供不超过10人天/年的安全专家现场应急响应。

线上钉钉、邮件告警：实现告警信息通过钉钉、邮件报表通知。

服务报告输出：每周提供监控到的安全隐患汇总统计（Excel格式），按季输出《云上资产自动化安全监控服务报告》。

**工作输出：**

《xx自动化监控服务风险周报表》

《xx季度-云上资产自动化安全监控服务报告》

**（四）安全培训服务**

**概述：**结合省委编办信息安全的实际情况和需求，对业务运维及技术人员进行1天的云上安全现场培训服务。

**工作目标：**进行省委编办网络及信息安全人员安全意识和技能培训，开展云安全产品实操培训，提升业务运维及技术人员安全意识和技能。

**工作内容及要求：**

应根据省委编办网络信息安全的实际情况和需求，提供全办范围内业务运维及技术人员的网络与信息安全培训，培训内容包括政务行业内外网络安全态势和案例、法律法规等安全意识培训，以及云上安全产品原理等安全技术培训。培训方式包括现场培训和远程培训两种方式相结合。

现场培训应提供讲解授课方式，远程培训应提供钉钉直播方式，可采用不定期开放方式提供，具体培训时间、形式和场地由省委编办确定。

**七、项目质量保证**

项目管理服务主要包括制定服务工作计划、服务流程、维护项目服务工作管理、维护服务的质量监督控制、对维护过程中的各种情况进行处理和维护跟踪、评审紧急审计解决方案、与用户的沟通交流，及与用户授权第三方交流等。

**（一）项目月报**

项目经理应在下个月的10号前提交本月的安全运维服务月报，月报发送指定的项目接口人，送抄双方相关责任人。

月报内容分四个层次对本月的工作内容进行汇报：

**1、本月工作概述，**说明本月的安全现状、重点工作、取得的成绩，上月遗留工作的处理及本月所遇到的主要问题，要求文字简洁、重点突出；

**2、本月主要工作内容，**根据项目各项工作的分类，将本月所完成的工作内容、实施步骤、使用方法进行详细说明 ，列出各项工作所遇到的问题，并给予解决建议；

**3、下个月工作安排，**将本月未完成的工作内容，项目实施计划表中计划的内容，以及项目领导要求的内容，写入下个月工作安排，工作安排应具体化，指明各项子任务实施内容，并写明预期的目标；

**4、月报附件，**对本月工作中的重点问题、专题工作或内容较多的部分作为附件或列在月报的最后章节，以方便实施层工作人员参考。

**（二）项目周报**

项目周报由项目经理在本周的下星期一前提交，项目周报为本周所完成工作的主要说明，周报以邮件形式发送项目接口人，抄送所有项目干系人。

项目周报的内容：

**1、本周安全整体情况，**本周安全故障、风险隐患及安全事件情况；

**2、本周安全运营工作情况，**本周新开展工作的内容，进度及所取得的成果；

**3、风险及问题，**在本周工作中发现的问题及解决建议；

**4、下周工作安排，**本周未完成的工作，任务计划列表中计划的工作以及领导特别安排的工作，写入下周工作计划。下周工作计划应具体、可执行。

**八、项目验收要求**

**验收分项清单**

项目各类型服务的验收交付物如下:

|  |  |  |  |
| --- | --- | --- | --- |
| **项目服务** | **交付内容** | **交付物** | **交付物类型** |
| 安全运维服务 | 安全运维服务工作详情 | 《xx月安全运维服务报告》 | 文档 |
| 应急演练服务 | 安全事件应急演练过程记录 | 《xx应急处置预案》《xx应急演练实施方案》《xx应急演练脚本》 | 文档 |
| 安全监控服务 | 云上资产自动化安全监控 | 《xx自动化监控服务风险周报表》《xx季度-云上资产自动化安全监控服务报告》 | 文档、产品功能 |
| 安全培训服务 | 安全意识及技能培训 | 《xx安全培训教材》 | 文档 |

由省委编办组织专家组进行验收

**商务要求表**

|  |  |
| --- | --- |
| **▲供货时间（项目工期）及地点** | 合同签定后一年内完成项目服务，并进行项目验收；地点:采购人指定地点。 |
| **▲付款条件（明确是否需要履约保证金）** | 合同签订后20日内，支付合同总价格的50%；通过验收后20个工作日内支付合同总额的50%。 |
| **违约责任及争议解决方式** | 如无特别说明，按“浙江省政府采购合同主要条款指引”相关违约责任及争议解决方式内容。 |
| **售****后****服务** | **项目维护计划** | 投标方应向采购人提供招标文件中的所有功能要求的项目服务。若项目服务不符合招标文件要求，投标方有责任和义务进行补充修改并征得采购人同意后付诸实施。（1）投标方应本着认真负责的态度组织技术队伍，做好投标的整体方案并提出升级、维护、服务以及今后技术支持的措施计划和承诺。（2）投标方应允许采购人的工作人员参与项目服务的监督、测试、诊断及解决问题等各项工作。（3）投标方必须对提供的项目保证服务质量。（4）投标方必须提供5×8小时的远程电话技术支持服务及7×24小时的紧急业务支持服务。 |
|   | **响应情况** | 中标方应在2小时内以电话、远程支持、传真等方式响应，提供对应项目服务的响应支持。 |
|   | **技术培训** | 投标方应针对本项目提供项目服务范围内日常操作与维护相应的培训服务计划，培训需根据采购人的安排进行，提供详细说明培训的方式、地点、人数、时间等实质性内容。 |
| **履约能力** | **公司技术力量情况** | 1、具备国家信息安全漏洞共享平台CNVD技术组成员单位、国家网络与信息安全信息通报机制技术支持-优秀技术支持单位资质，须提供相关证明材料。（同时具备得2分，部分或不具备不得分）2、具备CNCERT网络安全应急服务支撑单位（国家级）资质，须提供相关证明材料。（具备得2分）3、具备ISO 9001 质量管理体系认证、ISO 20000 IT服务管理体系认证、ISO 27017 云安全管理体系认证、ISO 22301业务连续性体系认证、ISO 27701 隐私资讯管理体系认证、BS 10012 个人数据管理体系认证。（同时具备得1分，部分或不具备不得分） |
|   | **经验或业绩要求** | 自2016年1月1日以来类似成功项目业绩，提供合同复印件需加盖公章。**（每提供一个得一分，最高3分）** |

**标项4: 监理服务项目**

**一、****概述**

按照省委编办信息化项目建设目标和要求，遵循国家、省、市信息系统项目建设和监理的标准和规范，按照“四控、三管、一协调”的原则，依据项目建设合同和用户需求，对省委编办2020年信息化建设/运维项目（以下述清单为准）提供全过程监理及安全服务评估。

服务期1年，具体起止时间由采购人在签订合同时确定。

总体包括三大部分：

一是提供全过程监理服务：监理服务范围包括系统开发、软硬件购置、安装调试、系统测试、系统培训、试运行和验收，系统移交及相关文档起草和管理、绩效管理等项目建设各个环节。

二是提供咨询服务：协助省委编办编制2021年信息化项目建设方案及相关材料；配合进行项目档案整理，资料建档等工作。

三是提供服务符合性评估：针对评估项目制定评估方案，编制评估报告，针对评估发现的问题，提出整改建议等工作。

**二、采购内容**

提供监理及相关咨询服务的项目清单：

1. **对中共浙江省委机构编制委员会办公室2020年度信息化建设项目提供全过程监理服务，项目清单如下：**
2. 实名制系统升级改造项目
3. 网络安全项目
4. **服务期内提供咨询服务**

协助编制2021年度信息化项目建设方案及相关材料；配合进行项目档案整理，资料建档等工作。

1. **符合性评估服务项目：**
2. 云上安全运维项目
3. 机房租用项目

**三、****监理服务要求**

监理人员现场工作期间，相关办公所需设备（如电脑、打印机、扫描机）及耗材由监理单位自行准备，且需满足日常工作开展。

为确保项目顺利实施，采购人要求：监理工作人员在业主单位工作时，应遵守采购人相关规章和制度；监理公司投入的办公设备应满足工作需求；如经甲方及第三方查实，监理单位及监理人员与被监理单位发生非正常经济往来及其他徇私舞弊情况，甲方有权要求更换监理人员或更换全体监理项目班子，情况严重的，甲方有权终止合同；项目中标后按照承诺到位人员进场开展工作，项目施工期间不得随意变动。

本项目总监及监理人员应与中标确定的人员相一致，如监理人因特殊原因在监理过程中更换项目总监及监理人员的必须向甲方正式提交书面申请并获得甲方同意，更换的人员应具备相应资质。

监理公司和现场人员需与省委编办签署项相关保密协议。

**四、****监理服务内容**

1、协助建设单位完成合同条款的审核与修改工作

监理单位驻场后，根据建设单位的要求，参与建设单位与承建单位合同的讨论，协助建设单位完成项目合同的编写工作，提出监理修改建议。

2、协助建设单位建立相关项目管理制度

根据建设单位实际项目管理的需求，协助建设单位制定相关项目管理制度。

3、全程参与项目日常监理工作。

根据“四控、三管、一协调”的原则，开展相关项目的监理工作。

1）质量控制

监理部按照监理大纲的质量控制点，在各阶段实施时，要求承建单位作出组织和技术保障措施，经监理审查，用户单位审定后执行，必要时召集相关技术人员对项目进行技术评审。

（1）需求阶段

在项目前期，参与项目需求的讨论，从而保证了解各业务部门的详细需求，并就有关需求组织评审和确认工作。

（2）设计开发阶段

在项目设计开发过程中，协助用户方详细审核承建单位提出的实施的技术方案、开发路线、设计文档，督促审核承建单位开发过程中是否按标准规范执行等。

（3）实施阶段

在软件系统实施过程中，要求承建单位在交付实施版本前对系统进行全面测试，并参与系统测试，确保项目稳定有效的实施。

在设备采购实施过程中，监理单位现场验收相关采购设备，根据投标文件和采购合同要求核对了设备型号、数量、随机配件和文档及售后服务。在实地的上架加电工作进行了严格的监督，在加电测试后要求承建单位，向监理单位和建设单位提交相应的测试方案和自测报告，监理单位根据承建单位测试方案和测试报告，对设备进行严格的监测。

（4）试运行阶段

对试运行存在问题的修改情况进行跟进，组织相关人员对试运行期间修改完成的问题进行测试。

（5）培训阶段

督促承建单位按照合同规定，向建设单位提供相关的培训服务，并要求承建单位提供培训教程。审核培训教程的规范性，要求承建单位在培训方案中明确培训时间、培训质量、培训地点、培训人数，了解培训情况。

（6）验收准备阶段

审核承建单位提供的设备是否符合合同约定的各项要求；技术文档和工程管理资料是否完备；审核试运行期间所提问题的修改情况。

2）进度控制

在整个项目实施过程中，督促和审核承建单位提交的工程进度计划。

在项目一开始，建立详细的监理制度。定时对承建方的进度进行检查，审核承建单位提交的工程进度报告，检查计划进度与实际进度的差异，进行工程施工的动态管理、进度分析和调整，并不定期向建设方报告有关工程项目进度情况。当工期目标严重偏离时，及时指出，并提出对策建议，同时督促承建单位尽快采取措施。

3）成本控制

在合同款支付前，核实工程量，核定应支付的进度款，对项目成本进行控制。

4）变更控制

5）文档管理/信息管理

在本项目建设过程中，项目文档管理贯穿整个工程实施的各个阶段。结合相关规范对承建单位提交的文档进行审核。

6）安全管理

负责项目建设过程中所涉及的政府机密数据和资料的保护，保证不被非授权使用。负责项目建设施工过程中安全控制，确保不出现安全事故。

7）项目合同管理

跟踪检查合同的执行情况，确保承建单位按时履约；

对合同工期的延误和延期进行审核确认；

对合同变更、索赔等事宜进行审核确认；

根据合同约定，审核承建单位提交的支付申请，签发付款凭证。

8）组织协调

在项目实施过程中，项目协调工作的原则是：诚信、公正、科学、公平。组织协调工作将贯穿于项目建设的全过程，包括了对工程进度控制、工程质量控制、信息管理等方面的组织协调工作。本项目主要的组织协调方式为会议、协商和沟通。

**五、软件类项目监理**

（1）审核和确认项目建设过程中的各种关键技术方案；

（2）审核和确认承建单位的项目实施方案、项目计划和人员组成；

（3）审核和确认承建单位的项目质量保证计划、质量控制体系（含质量控制的关键性节点）；

（4）审核和确认承建单位的测试计划；

（5）审核和确认承建单位的项目进度计划和进度控制节点；

（6）应用软件开发的阶段性计划的审核和确认；

（7）对承建单位的开发质量进行审核；

（8）对源代码、开发文件进行移交验收；

（9）审核确认承建单位的培训计划；

（10）参与软件的功能测试，并提出监理测试意见；

（11）对项目实施进度进行实时跟踪，并要求承建单位对进度计划进行动态调整，以确保项目的阶段和总体进度目标的实现；

（12）当工期目标严重偏离时，应及时指出，并提出对策建议，同时督促承建单位尽快采取措施。

（13）审核承建单位提交的付款申请，将付款进度与项目质量与形象进度结合起来。

（14）跟踪检查合同的执行情况，确保承建单位按时履约；

（15）对合同工期的延误和延期进行审核确认；

（16）对合同变更、索赔等事宜进行审核确认；

（17）做好合同批复等各类往来文件的批复和存档；

（18）做好项目协调会、技术专题会的会议纪要；

（19）管理好实施期间的各类技术文档；

（20）监理通知；

（21）各种会议纪要；

（22）阶段性项目总结；

（23）审核承建方提交的技术文档是否符合项目验收要求。

（24）协助建设单位做好项目验收工作。

**六、协助用户日常性事务管理**

（1）协助用户单位历年信息化项目文档整理、归档工作。相应文档扫描、复印、存档，实行电子和纸质分别归档等工作（包括项目前期的建议书、可研报告、实施报告、相关批复文件、验收意见、项目相关标准、制度等除验收资料外的项目资料）。

（2）协助用户单位往年建设项目的审计、资料整理等工作。

（3）协助用户单位相关文件的复印、传真、传递、排版、打印，电话通知等日常办公事务。

（4）协助用户做好有关信息化项目其他事宜。

**七、监理服务准则**

遵照国家信息产业部《信息系统项目监理暂行规定》的有关规定，以“守法、诚信、公正、科学”的准则执业，维护建设方与承建方的合法权益。具体应做到：

（1）执行有关项目建设的法律、法规、规范、标准和制度，履行监理合同规定的义务和职责。

（2）不收受被监理单位的任何礼金。

（3）不泄漏所监理项目各方认为需要保密的事项。

（4）遵守国家的法律和政府的有关条例、规定和办法等。

（5）坚持公正的立场，独立、公正地处理有关各方的争议。

（6）坚持科学的态度和实事求是的原则。

（7）在坚持按监理合同的规定向采购人提供技术服务的同时，帮助被监理者完成起担负的建设任务。

（8）不泄漏所监理的项目需保密的事项。

**八、监理服务遵照的依据**

（1）国家工信部和我省有关信息系统项目建设和监理管理规范；

（2）采购人与项目承建单位签订的合同；

（3）采购人与监理单位签订的监理合同；

**九、信息化项目服务符合性评估内容：**

1、前期基础调研

针对政府投资信息化项目的全生命周期进行基础调研，含现场走访、资料查阅、调查问卷等方式，了解信息化项目管理的关键环节、信息化项目的种类及各自业务特征，做为制定科学合理的项目评估方案和评估参数表的基础。

2、制定符合性评估方案，设计信息化项目评估指标体系

基于前期基础调研的诊断及成果，以及类似项目的评估经验借鉴，完成评估方案的制定，并据此设计信息化项目的评估指标体系（含评估参数、权重、数据来源等）。

3、依据评估方案，对用户抽取的信息化项目进行符合性评估

依据评估方案，对信息化项目进行符合性评估，包括但不限于以下内容：

①对项目建设的规范性进行评估：如立项、采购、建设内容的一致性和延续性、进度和变更控制、资金支付、项目验收等；

②对项目的运行情况进行评估：如维保经费、台帐、设备现场标识、安全性、用户培训情况等；

③对项目的运行进行评估：如系统对业务的支撑作用、管理成本节约、便民服务、政府资源共享等。

4、根据评估情况，编制评估报告

结合项目的估情况，对编制项目的评估报告，内容包括：项目基本概况、符合性评估结论、评估中发现的问题、评估建议等。

5、针对评估发现的问题，提出整改建议，并进行跟踪处理

依据评估结果，提出独立客观的整改建议，协助甲方对项目整改情况进行跟踪，形成PDCA循环，直至问题关闭。

**十、其他要求**

1、供应商应在响应文件中提供但不限于以下内容：

（1）监理服务大纲

（2）关键点的特殊控制方案

（3）项目理解及合理化建议

（4）质量控制方案

（5）进度控制方案

（6）项目成本/投资控制方案

（7）变更控制方案

（8）合同、安全和信息管理方案

（9）其他与本项目评审评分有关的资料等。

2、监理工作相关管控软件：如有，请提供相关行业软件证明材料。

**十一、项目组人员个人能力情况（与评分标准相对应）**

1、项目总监理工程师（4分）：

要求具备本单位十年(含)以上信息化监理相关工作经验并具有信息系统监理师证书( 1分)，还需具有人力资源和社会保障部门颁发的数据库系统工程师证书（ 0.5分），具有人力资源和社会保障部门颁发的信息系统项目管理师证书（ 0.5分），具有人力资源和社会保障部门颁发的一级建造师（机电工程专业）证书（0.5 分），中国工程咨询协会颁发咨询工程师（投资）证书（0.5 分），中国信息安全测评中心颁发注册信息安全工程师（CISE）证书（0.5 分），全国互联网应用水平考试管理办公室颁发程序员（高级）（ 0.5分）；

2、项目总监代表（4分）：

要求具备本单位五年(含)以上信息化监理相关工作经验并具有信息系统监理师证书(1分)，中国计算机软件专业技术资格和水平考试委员会颁发的高级程序员（1分），人力资源和社会保障部门颁发的软件评测师（0.5分），人力资源和社会保障部门颁发的信息系统项目管理师（高级）（0.5分），人力资源和社会保障部门颁发数据库系统工程师（1分）。

3、监理服务团队（ 6分）：

监理服务团队组成人员（除总监、总监代表外）具备本单位六年(含)以上信息化监理相关工作经验并具有信息系统监理师的同时具有以下证书人员：具有人力资源和社会保障部门颁发（培训等机构颁发的无效）的网络工程师证书（0.5分）、系统集成项目管理工程师（0.5分）、软件评测师（0.5 分）、中国计算计软件专业技术资格和水平考试委员会颁发的高级程序员（1分）、中国软件评测中心颁发软件性能测试高级工程师证书（1分）、工业和信息化部人才交流中心颁发全国计算机大数据处理专业人才（高级）证书（1 分）、工业和信息化部教育与考试中心颁发软件工程造价师（1分）、工业和信息化部信息中心颁发的软件架构设计（高级）证书（0.5分）。

**提供以上公司、人员相关证书复印件及人员近三个月在本公司缴纳的社保证明，开标时原件备查。**

**商务要求表（与评分标准相对应）**

|  |  |
| --- | --- |
| **▲供货时间（项目工期）及地点** | 交货时间：合同签订后10天内派驻监理入员入场至被监理的项目结束截止。交货地点：用户指定地点。 |
| **▲付款条件** | 合同签订后10个工作日内，支付合同总额的80%，项目建设完成，提交该项目全部报告材料，并通过正式验收后10个工作日，甲方在履行财政相关资金审批手续后10个工作日内，甲方支付余款。 |
| **违约责任及争议解决方式** | **按“第五章 浙江省政府采购合同主要条款指引”相关违约责任及争议解决方式内容。** |
| **售****后****服务** | **项目维护计划及响应情况（5分）** | 服务期：从签订监理合同开始，直到项目终验合格结束。1、评审承建单位在系统质保期内的服务计划，给出评审意见。2、抽查承建单位在系统质保期内履行服务计划、服务的响应时间的情况。3、协助采购人确认承建单位在系统质保期后的后续服务能力。4、协助采购人在系统质保期内做好定期的系统全面检查，确保系统运行正常。5、在质保期内做好各承建单位和采购人之间的协调工作。 |
| **技术培训** | 无。 |
| **履约能力** | **公司综合实力情况（5分）** | 具有：1. 省（或国家）保密局颁发涉密信息系统集成资质【工程监理、系统咨询（1分）】；
2. 工商行政管理部门确认的“守合同、重信用”企业称号，2A级（含）证书（1分）。

3、质量管理体系认证证书（0.5分）；4、信息安全风险评估服务资质证书（0.5分）；5、ITSS信息技术服务咨询设计标准符合性证书（0.5分）；6、信息安全管理体系认证证书（0.5分）；7、参与过财政组织的行政事业单位定点绩效评价服务的（提供入围公告及绩效评价合同复印件或者用户证明）（1分）**(注：同一事项重复计算，满分5分，开标时提供合同原件备查）** |
| **投标人经验或业绩要求（5分）** | 提供2016年1月1日以来行政事业单位同类项成功案例合同复印件**（每提供1个得1分，满分5分，开标时提供合同原件备查）** |

**第五章 浙江省政府采购合同主要条款指引**

合同编号：

 确认书号：

**甲方**（采购人）：

**乙方**（供应商）：

**鉴证方:** 浙江省政府采购中心

甲、乙双方根据浙江省政府采购中心关于项目编号为 的（标项及名称）项目公开招标的结果，签署本合同。

**一、项目内容及合同价格**

金额单位：元

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 项目名称 | 技术需求 | 数量 | 单价 | 总价 |
|  | 详见项目对应招投标文件 |  |  |  |
| 合 计 |  |  |
| 合同总价大写： 小写：￥ |

注：1.项目具体技术需求及采购人地址等详见招标文件、投标文件以及询标记录。

　2.以上合同总价包含项目达到预期使用效果所需的一切费用。

**二、技术资料**

1.乙方应按招标文件规定的时间向甲方提供使用项目的有关技术资料。

2.没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

**三、知识产权**

乙方应保证所提供的货物或其任何一部分均不会侵犯任何第三方的知识产权。

**四、产权担保**

乙方保证所交付的货物的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

**五、转包或分包**

不允许转包。

允许分包部分 。

如乙方将项目转包或将不允许分包部分就行了分包，甲方有权解除合同，没收履约保证金并追究乙方的违约责任。

**六、质保期和履约保证金**

1.质保期年。（自项目验收合格交付使用之日起计）

2.履约保证金元。[履约保证金交至采购人处，在合同约定交货验收合格满（ ）个月之日起5个工作日内无息退还]

**七、项目工期及实施地点**

1.交货期：

2.实施地点：

**八、货款支付**

 付款方式：

**九、税费**

本合同执行中相关的一切税费均由乙方负担。

**十、质量保证及售后服务**

详见招标文件。

**十一、调试和验收**

详见招标文件。

**十二、货物包装**

详见招标文件。

**十三、违约责任**

1.甲方无正当理由拒收验收项目的，甲方向乙方偿付拒收合同总价的百分之五违约金。

2.甲方无故逾期验收和办理合同款项支付手续的,甲方应按逾期付款总额每日万分之五向乙方支付违约金。

3.乙方逾期交付项目的，乙方应按逾期交付项目总额每日千分之六向甲方支付违约金，由甲方从合同款项中扣除。逾期超过约定日期10个工作日不能交付的，甲方可解除本合同。乙方因逾期交付或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

4.乙方所交的货物品种、型号、规格、技术参数、质量不符合合同规定及招标文件规定标准的，甲方有权拒收该货物，乙方愿意更换货物但逾期交货的，按乙方逾期交货处理。乙方拒绝更换货物的，甲方可单方面解除合同。

5.解除合同应按《浙江省合同管理办法》向财政备案。

**十四、不可抗力事件处理**

1.在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2.不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3.不可抗力事件延续120天以上，双方应通过友好协商，确定是否继续履行合同。

**十五、诉讼**

双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向甲方所在地法院起诉。

**十六、合同生效及其它**

1.合同经甲、乙、鉴证方三方签名并加盖单位公章后生效。

2.合同执行中涉及采购资金和采购内容修改或补充的，须经采购中心、财政部门审批，并签书面补充协议，经报政府采购监督管理部门备案后，方可作为主合同不可分割的一部分。

3.招标文件、投标文件与本合同具有同等法律效力。

4.本合同未尽事宜，遵照《合同法》有关条文执行。

5.本合同一式六份，具有同等法律效力，甲、乙、鉴证三方各执二份。

甲方（盖章）：

地址：

法定（授权）代表人：

签名日期： 年 月 日

乙方（盖章）：

地址：

开户行：

开户帐号：

法定（授权）代表人：

签名日期： 年 月 日

合同鉴证方（盖章）:

法定代表人或主要负责人:

鉴证日期: 年 月 日

**第六章 投标文件格式附件**

附件1**：** 正本或副本

项目名称

项目编号：ZZCG2020D-GK-107（标项 ）

**资**

**质**

**文**

**件**

投标人全称：

地 址：

时 间：

**1、资质文件目录**

（1）投标声明书 (格式见附件，含重大违法记录声明)；

（2）法定代表人授权委托书(格式见附件)；

（3）提供有效的营业执照复印件并加盖公司公章；事业单位的，则提供有效的《事业单位法人证书》副本复印件并加盖单位公章；自然人的，则提供有效的身份证复印件并签字；

（4）提供有效的依法缴纳税收证明（完税凭证或税务部门出具的证明）；

（5）提供有效的依法缴纳社会保障资金证明（缴纳凭证或人社部门出具的证明）；

（6）联合投标协议书（若需要）;

（7）联合投标授权委托书（若需要）;

（8）提供采购公告中符合投标人特定条件要求的有效的其他资质复印件并加盖公司公章及需要说明的资料。

附件2：

**声 明 书**

致浙江省政府采购中心：

（投标人名称）系中华人民共和国合法企业，经营地址。

我（姓名）系（投标人名称）的法定代表人，我方愿意参加贵方组织的（招标项目名称）（编号为ZZCG2020D-GK-107）的投标，为此，我方就本次投标有关事项郑重声明如下：

1.我方已详细审查全部招标文件，同意招标文件的各项要求，包括疫情期间采取的各项应急开标措施。

2.我方向贵方提交的所有投标文件、资料都是准确的和真实的。

3.若中标，我方将按招标文件规定履行合同责任和义务。

4.我方不是采购人的附属机构；在获知本项目采购信息后，与采购人聘请的为此项目提供咨询服务的公司及其附属机构没有任何联系。

5.投标文件自开标日起有效期为90天。

**6.我方参与本项目前3年内的经营活动中没有重大违法记录；**

7.我方通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询，未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

8.以上事项如有虚假或隐瞒，我方愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

法定代表人签名（或签名章）： 日 期：

投标人全称（公章）：

附件3：

**法定代表人授权委托书**

浙江省政府采购中心：

我（姓名）系（投标人名称）的法定代表人，现授权委托本单位在职职工 （姓名）为授权代表，以我方的名义参加项目编号：项目名称： 项目的投标活动，并代表我方全权办理针对上述项目的投标、开标、评标、签约等具体事务和签署相关文件。我方对授权代表的签名事项负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。授权代表在授权书有效期内签署的所有文件不因授权的撤销而失效。

授权代表无转委托权，特此委托。

授权代表签名： 职务：

授权代表身份证号码：

法定代表人签名（或签名章）： 职务：

投标人全称（公章）： 日 期：

附件4：

**联合投标协议书**

甲方：

乙方：

（如果有的话，可按甲、乙、丙、丁…序列增加）

各方经协商，就响应 组织实施的编号为号的招标活动联合进行投标之事宜，达成如下协议：

一、各方一致决定，以 为主办人进行投标，并按照招标文件的规定分别提交资格文件。

二、在本次投标过程中，主办人的法定代表人或授权代理人根据招标文件规定及投标内容而对招标方和采购人所作的任何合法承诺，包括书面澄清及响应等均对联合投标各方产生约束力。如果中标并签订合同，则联合投标各方将共同履行对招标方和采购人所负有的全部义务并就采购合同约定的事项对采购人承担连带责任。

三、联合投标其余各方保证对主办人为响应本次招标而提供的产品和服务提供全部质量保证及售后服务支持。

四、本次联合投标中，甲方承担的工作和义务为:

乙方承担的工作和义务为：

五、有关本次联合投标的其他事宜：

六、本协议提交招标方后，联合投标各方不得以任何形式对上述实质内容进行修改或撤销。

七、本协议签约各方各持一份，并作为投标文件的一部分。

|  |  |
| --- | --- |
| 甲方单位： （公章）法定代表人： （签章）日 期： 年 月 日 | 乙方单位： （公章）法定代表人： （签章）日 期： 年 月 日 |

附件5：

**联合投标授权委托书**

 本授权委托书声明：根据 与签订的《联合投标协议书》的内容，主办人的法定代表人现授权 为联合投标代理人，代理人在投标、开标、评标、合同谈判过程中所签署的一切文件和处理与这有关的一切事务， 联合投标各方均予以认可并遵守。

 特此委托。

授权人（签名）：

日期： 年 月 日

授权代表（签名）；

日期： 年 月 日

|  |  |
| --- | --- |
| 联合体甲方单位： （公章）法定代表人： （签章）日 期： 年 月 日 | 联合体乙方单位： （公章）法定代表人： （签章）日 期： 年 月 日 |

附件6**：**  正本或副本

项目名称

项目编号：ZZCG2020D-GK-107（标项 ）

**技**

**术**

**及**

**商**

**务**

**文**

**件**

投标人全称：

地 址：

时 间：

2、**技术及商务文件目录**

（1）评分对应表（格式见附件，主要用于评委对应评分内容）

（2）投标项目明细清单（含货物、服务等）；

（3）技术响应表（格式见附件）；

（4）项目总体解决方案（可包含且不限于对项目总体要求的理解、项目总体架构及技术解决方案等）；

（5）项目实施计划（可包含且不限于保证工期的施工组织方案及人力资源安排、项目组人员清单等）；

（6）列入政府采购节能环保清单的证明资料（若有）；

（7）商务响应表（格式见附件）；

（8）售后服务计划（可包含且不限于对用户故障的响应、处理、定期巡检、备品备件、常用耗材提供、驻点人员情况等）；

（9）技术培训计划（若有）；

（10）投标人履约能力（可包含且不限于技术力量情况、投标人各项能力证书）；

（11）案例的业绩证明（投标人业绩情况一览表、合同复印件等）；

（12）投标方认为需要的其他文件资料。

附件7：

**评分对应表**

投标人全称（公章）： 标项：

|  |  |  |
| --- | --- | --- |
| 评分项目 | 投标文件对应资料 | 投标文件页码 |
| 对应第三章评分办法及评分标准（报价除外） |  |  |
| …… |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

授权代表签名： 日期：

附件8：

**投标项目明细清单**

投标人全称（公章）： 标项：

货物类

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 品牌 | 规格型号 | 单位及数量 | 性能及指标 | 产地 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

服务类

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务内容 | 服务人员数量 | 工作量 |
|  |  |  |  |
|  |  |  |  |

注：在填写时，如上表不适合本项目的实际情况，可在确保投标明细内容完整的情况下，根据上表格式自行划表填写。

授权代表签名： 日期：

附件9：

**技 术 响 应 表**

投标人全称（公章）： 标项：

|  |  |  |
| --- | --- | --- |
| 招标文件要求 | 投标文件响应 | 偏离情况  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

注：投标人应根据投标设备的性能指标、对照招标文件要求在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”。

授权代表签名： 日 期：

附件10：

**项目组人员清单**

投标人全称（公章）： 标项：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 姓名 | 职务 | 专业技术资格 | 证书编号 | 参加本单位工作时间 | 劳动合同编号 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：在填写时，如本表格不适合投标单位的实际情况，可根据本表格式自行划表填写。

授权代表签名： 日 期：

附件11：

**商务响应表**

投标人全称（公章）： 标项：

|  |  |  |  |
| --- | --- | --- | --- |
| 项目 | 招标文件要求 | 是否响应 | 投标人的承诺或说明 |
| 供货时间（项目工期）及地点 |  |  |  |
| 付款条件 |  |  |  |
| 违约责任及争议解决方式 |  |  |  |
| 项目维护计划 |  |  |  |
| 响应情况 |  |  |  |
| 本地化服务要求 |  |  |  |
| 技术培训 |  |  |  |
| 公司技术力量情况 |  |  |  |
| 经验或业绩要求 |  |  |  |
| …… |  |  |  |

授权代表签名： 日期：

附件12：

**投标人业绩情况一览表**

投标人全称（公章）：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 采购单位名称 | 设备或项目名称 | 采购数量 | 单价 | 合同金额（万元） | 附件页码 | 采购单位联系人及联系电话 |
| 合同 | 验收报告 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 备注 | 提供投标人同类项目合同复印件、用户验收报告（如有）。 |

授权代表签名：　　　　　 时 间：

附件13**：**  正本或副本

项目名称

项目编号：（标项 ）

**报**

**价**

**文**

**件**

投标人全称：

地 址：

时 间：

3、**报价文件目录**

（1）投标报价明细表（见附件14）；

（2）投标人针对报价需要说明的其他文件和说明（格式自拟）；

（3）小微企业声明函（见附件15）；

（4）残疾人福利企业声明函（见附件16）。

附件14：

**投 标 报 价 明 细 表**

投标人全称（公章）：

招标编号及标项：

|  |
| --- |
| **货物类** |
| **货物****名称** | **品牌** | **产地** | **规格****型号** | **数量** | **单价****（元）** | **总价（元）** | **制造商情况** |
| **是否小微企业** | **企业全称** |
| **…** |  |  |  |  |  |  |  |  |
| **服务类** |
| **服务内容** | **服务人员数量** | **工作量** | **单价****（元）** | **总价（元）** | **制造商情况** |
| **是否小微企业** | **企业全称** |
| **…** |  |  |  |  |  |  |
| **小微企业价格合计金额大写： 小写： ￥** |
| **投标总价合计金额大写： 小写： ￥** |
| 备注 | 1.此表应按项目的明细情况列项填报,在填写时，如上表不适合本项目的实际情况，可在确保投标明细内容完整的情况下，根据上表格式自行划表填写。2.报价要求：项目费用包括项目实施所需的工程费、工时费、服务费、运输费、安装调试费、税费及其他一切费用。3.报价中不允许出现报价优惠等字样（明细出现“0”元，视同赠送）,投标总价合计金额应与明细报价汇总相等。**4.小微企业价格合计金额应与“制造商为小微企业”的明细报价汇总相等（如有错误修正，以修正后的明细报价为准），评标委员会按前附表“小微企业有关政策”要求对小微企业价格进行确认，并对符合要求的小微企业价格部分给予价格扣除。**5**.**开标时，现场工作人员当众拆封，并宣布投标人名称、投标总价合计金额。 |

授权代表签名： 日期：

附件15：

**小微企业声明函**

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库〔2011〕181号）的规定，本公司为（请填写：小型、微型）企业。即，本公司同时满足以下条件：

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

2.本公司参加单位的项目采购活动提供本企业制造的货物，由本企业承担工程、提供服务，或者提供其他（请填写：小型、微型）企业制造的货物。本条所称货物不包括使用大型企业注册商标的货物。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

 企业名称（盖章）：

 日 期：

**备注说明：**

1.《小微企业声明函》中，须同时满足以上两个条件。若投标人提供非本企业制造的货物，其制造商也须为小型、微型企业；

2.若联合体投标时，联合体各方均为小型、微型企业的，联合体各方均须提供《小微企业声明函》；联合体其中一方为小型、微型企业的，联合协议中须约定小型、微型企业的协议合同金额占到联合体协议合同总额30%以上。

附件16：

**残疾人福利性单位声明函**

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

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

 单位名称（盖章）：

 日 期：