浙江省人力社保厅网络安全优化项目

项目编号：ZZCG2020D-GK-119

**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** 6](#_Toc496796636)

[**第三章评标办法及评分标准** 22](#_Toc496796637)

[**第四章招标需求** 25](#_Toc496796638)

[**第五章浙江省政府采购合同主要条款指引** 55](#_Toc496796639)

[**第六章投标文件格式附件** 60](#_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-119**

**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** | **浙江省人力社保厅网络安全优化项目** | **1** | **批** | **500** |

**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:不允许联合体投标**

**五、获取采购文件：**

1 2020年7月2日至2020年7月27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7月27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7月28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） | 陈玮洁 | 0571-88907785 | 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：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **采购单位** | 浙江省人力资源和社会保障信息中心 | | | |
| **地 址** | 杭州市体育场路538号金祝大厦11楼 | | | |
| **咨询事项** | **联系人** | **联系方式** | **传真** | **备注** |
| 采购需求等 | 朱国耀 | 0571-85116991 |  |  |

**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  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****4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 | 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 |

**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:****浙江省人力社保厅网络安全优化项目**

# 一、采购内容

2019年我厅已经根据省委网信办《关于开展专网安全管控体系建设试点工作的函》要求，进一步提升了人力社保专网安全保障能力，初步通过资产摸底核查，建立终端、服务器、网络设备、安全设备等各类信息化资产清单，明确资产名称、位置、用途、管理人员等各类资产关键属性，建立了省人力社保网络安全管理核心平台基础功能，初步完成安全运行工作机制，同时初步实现信息资产清晰、风险隐患可见、终端安全可控的安全管理支撑体系首阶段目标。

但是，随着人力社保信息化向“大整合、高共享、深应用”以及浙江省政府“最多跑一次”改革，数据安全问题日益突出，急需在原有省人力社保网络安全管理核心平台基础上，进一步完善功能，整合数据，对接外部第三方网络安全通报预警信息，探索开展基于大数据分析的网络安全风险智能分析预警，进一步加强省人力社保厅安全风险监测、分析和防护能力及应用、数据安全防护能力，确保网络整体安全。

# （一）建设目标

在前期已初步建成的网络安全管理支撑体系和安全防护手段基础上，本项目进一步优化浙江省人力资源和社会保障厅网络安全管理支撑体系和安全技术保障体系。

安全管理支撑体系优化重点是完善网络安全管理核心平台、提升安全智能分析预警、和网络安全协调指挥能力，提高省人力社保厅安全风险监测、分析和防护水平。通过省人力社保网络安全管理核心平台和数据分析技术，整合省人力社保厅现有的内网终端安全日志、网络流量安全日志等安全源数据，进行安全源数据挖掘分析及风险建模,同时结合外部第三方网络安全通报预警信息的有效补充，初步实现内外网资产统一管理、风险统一监测的安全管理支撑体系。

（1）完善现有网络安全管理核心平台网络安全综合展示功能，增加外网网页篡改、病毒木马、安全漏洞、网络攻击等安全风险、事件展示。建设应急协调联动子系统，作为网络安全管理核心平台的统一接口功能，在确保网络安全管理核心平台相对稳定的基础上，对接安全智能分析预警的安全数据和网络安全协调指挥的风险、事件等数据，并确保接口的开放性，为今后其他平台对接做好预留。

（2）提升安全智能分析预警能力，实现对省人力社保厅原有网络安全管理核心平台内网终端安全日志源数据、网络流量安全日志源数据的整合利用，在原有平台数据基础上对安全源数据进行挖掘分析和风险建模，实现内网安全风险的智能分析和安全应用。

（3）根据省委网信办《浙江省网络安全协调指挥平台建设指南》的要求，提升网络安全协调指挥能力，实现省人力社保厅外网的实时监测、态势感知、信息通报等业务功能。

安全技术保障体系优化重点通过建设服务器安全加固、漏洞风险监测、数据库安全防护、防火墙、上网行为管理等技术手段，提升安全防护能力。

（1）服务器安全加固扩容：根据人社业务系统资产数量增加授权数，为服务器提供外设管控、文件审计、违规外联检测与阻断等主机安全加固防护。

（2）漏洞风险监测：根据省人力社保厅的已知资产自动、快速、准确检测发现省厅的资产的漏洞，帮助安全管理人员更快速、更全面、更智能地管理网络资产安全漏洞风险。

（3）数据库安全防护：增加数据库防护系统授权，对重要数据库操作行为进行安全审计记录和安全防护。

（4）防火墙：增加部署防火墙，加强安全防护。

（5）上网行为管理：加强省厅的政务外网上网终端的上网行为的管理。

# （二）采购内容

|  |  |  |
| --- | --- | --- |
| 序号 | 设备/软件名称 | 数量 |
| 1 | 完善现有网络安全管理核心平台 | 1套 |
| 2 | **安全智能分析预警（核心产品）** | 1套 |
| 3 | 网络安全协调指挥 | 1套 |
| 4 | 服务器安全加固 | 1套 |
| 5 | 漏洞风险监测 | 1台 |
| 6 | 数据库防护系统 | 1套 |
| 7 | 防火墙 | 1台 |
| 8 | 上网行为管理系统 | 1台 |

# （三）详细技术要求

省人力社保厅网络安全体系由安全资源层、管理支撑层、综合展示层组成，按照“积极防御、综合防范、技管并重”的发展思路，建立以安全防护基础设施建设为支撑，以安全管理体系为引领，以安全计算环境、安全区域边界、安全通信网络安全技术手段为主体，以组织领导和法规标准为保证，以安全防护专业力量建设为基础的网络安全管控体系。如图1所示。



图1 浙江省人力社保厅网络安全体系建设示意图

网络安全综合展示系统通过风险综合展示、事件综合展示、业务系统综合展示、设备综合展示、安全管理全流程动态展示等模块，采集来自网络安全管理核心平台的数据，通过精准定位和数据分析，从不同维度立体展示全省人社系统专网安全态势，真正实现全省安全态势展现标准化和一体化。

网络安全管理核心平台是管理员日常管理的主要工作界面，对内采集安全智能分析预警安全风险和事件数据，对外采集来自公众服务网部署的网络安全协调指挥安全风险和事件数据，汇总后在网络安全综合展示子系统进行展示。

网络安全管理核心平台将采集到的安全风险和事件日志，通过自动或人工确认的方式，和资产、安全管理相关人员组织架构相关联，按照已制定形成的风险和事件处置流程，实现省人社系统网络安全管理的规范化和标准化。

通过内网部署的安全智能分析预警实现对海量数据进行纵向分析和横向关联，发现数据中隐藏的安全风险，实现威胁发现、精准预警和态势感知。

通过外网部署的网络安全协调指挥实现对外网及时发现、识别和监测恐怖组织、黑客组织和不法分子的攻击活动、攻击行为、攻击方法，对网络空间安全相关信息进行汇聚融合，从不同视角感知网络安全威胁。

网络安全技术保障体系包括漏洞风险监测、数据库防护、防火墙、上网行为管理等技术手段建设，做到设备入网时实时开展合规检查、阻断非法网络边界、监测终端应用行为、监控敏感数据流转，严防数据泄露安全风险。

具体指标要求如下：

* + - 1. 完善现有网络安全管理核心平台指标要求

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| ▲总体要求 | 在现有的省人力社保厅网络安全管理核心平台基础上，按省委网信办《关于开展专网安全管控体系建设试点工作的函》要求进一步拓展平台功能，完善现有网络安全管理核心平台网络安全综合展示模块，增加外网网页篡改、病毒木马、安全漏洞、网络攻击等安全风险、事件展示；建设应急协调联动子系统，作为网络安全管理核心平台的统一接口功能，在确保网络安全管理核心平台相对稳定的基础上，对接安全智能分析预警的安全数据和网络安全协调指挥的风险、事件等数据，并确保接口的开放性，为今后其他平台对接做好预留。 |
| **完善网络安全综合展示模块** | |
| **指标项** | **指标要求** |
| 完善综合展示首页 | 支持对新增风险类型：网页篡改、病毒木马、安全漏洞、网络攻击等风险的统计和展示，支持风险详情的深入查询；支持对设备、业务系统、新增风险、风险处理、可疑行为的总数、今日变化数量进行统计，支持对新增风险分类和地区情况的统计和展示，支持对新增风险实时预警；支持对新增风险历史数据信息的展示，支持安全风险指数指标。 |
| 完善风险总览 | 支持通过地图体现各区域的数据接入状态和当前的新增风险：网页篡改、病毒木马、安全漏洞、网络攻击等风险的存在情况；支持风险发生时间的曲线图统计；支持风险类型的柱状图、饼状图统计；支持按近一日、近一周、近一月、近一年进行数据筛选查询统计。 |
| 完善资产总览 | 支持设备类型、操作系统类型、数据库类型、所属等保大类等的统计和展示。 |
| 新增成效总览 | 支持通过地图体现各区域的数据接入状态，反映各区域的数据上报情况；支持对新增风险：网页篡改、病毒木马、安全漏洞、网络攻击等风险的数量统计和处理率统计；支持新增高危风险、中危风险、低危风险的处理数top5排名；支持高危、中危、钉办流程的已完成、未完成、完成率的统计，以及各个区域的处理率排名。支持建设成效安全系统建设率的排名统计。 |
| **建设应急协调联动子系统** | |
| **指标项** | **指标要求** |
| ▲总体要求 | 基于浙政钉开发移动办公应急响应模块，作为网络安全管理核心平台的统一接口功能，在确保网络安全管理核心平台相对稳定的基础上，对接安全智能分析预警的安全数据和网络安全协调指挥的风险、事件等数据，并确保接口的开放性，为今后其他平台对接做好预留。 |
| 首页模块 | 支持网络安全指数评分（优良中差）的展示；支持统计概况，包括但不限于设备总数、业务系统总数、风险总数、风险处理数、可疑行为数的统计，以及今日变化统计；支持指数地图展示，通过地图可查看所属区域的网络安全指数级别（优良中差），支持选择地市查看该地市的详情数据；支持风险趋势统计，可查看近一月的发现风险、处理风险的数量统计，并且也可查看近一月的高危风险、中危风险、低危风险的数量统计；支持地区统计，可查看所有市、县的安全指数、风险数、可疑行为数、设备数、业务系统数、风险处理数等。 |
| 工作管理模块 | 支持工作流程管理，包括待办事宜、已办流程、办结流程、我的抄送等模块，可查看流程内容，处置和抄送风险流程情况，数据内容与安全管理支撑平台实时同步。  支持待处理风险管理，可查看风险详情，内容包括风险类型、安全级别、处理状态、发生时间、风险描述、关联业务系统名称、责任单位部门、责任人、厂商、厂商责任人、设备IP、设备MAC、设备类型等；可支持风险转流程操作，并转为风险流程处理环节；支持超时告警功能，可操作查看、删除、钉办等功能；支持安全通知功能的查看功能。 |
| 个人配置管理模块 | 支持个人信息的展示，包括所属单位部门、人员姓名、账户名等信息；支持账户密码的修改。 |
| 对接接口要求 | 实现安全智能分析预警安全数据接口对接。实现网络安全协调指挥的风险、事件等数据接口对接，并确保接口的开放性，为今后其他平台对接做好预留。 |

* + - 1. 安全智能分析预警指标要求

|  |  |  |
| --- | --- | --- |
| **指标项** | | **指标要求** |
| ▲总体功能 | | 实现省人力社保厅内网终端安全日志、网络流量安全日志的整合利用，终端安全日志信息包括终端人员访问、操作系统安全配置、进程、端口、流量、连接日志信息、网络安全日志信息包括人员访问、协议、流量、源IP、目标IP、访问端口、应用进程日志信息。并且对这些安全日志进行挖掘分析和风险建模，构建内网终端安全、网络流量安全分析能力。 |
| 安全数据采集 | | 1. 客户端数据采集   支持对接人社现有的终端安全客户端软件，采用集成插件和主动连接的方式，由数据采集探针自动采集终端产生的安全监测和日志数据。具体包括终端基础配置数据、审计数据、实时行为数据三大类。终端数据采集方式支持实时采集和间隔采集方式。   1. 第三方安全系统数据采集   支持包括已部署实施的网络安全管理核心平台、数据合规应用子系统、综合日志审计系统业务数据采集和应用分析，实现对网络和通信安全分析、数据和使用安全分析的原始数据支持。  3）数据采集要求：根据不同的数据来源、数据类型，实现对目标源数据采集。具体功能包括：  数据采集：部署在所要采集的目标数据源上，用于主动式数据采集。  数据推送：支持接收目标数据源推送的数据，用于被动式数据采集等功能。  数据总线管理：对数据采集任务、采集过程进行状态监测。 |
| 安全流量数据采集探针：标准机架式设备， CPU≥8核；内存≥16G；硬盘≥1T，安全流量数据采集探针。 |
| 终端安全数据采集探针：标准机架式设备， CPU≥8核；内存≥16G；硬盘≥1T，终端安全数据采集探针。 |
| 安全日志数据采集探针：标准机架式设备， CPU≥8核；内存≥16G；硬盘≥1T，安全日志数据采集探针。 |
| 人社安全综合展示子系统接口对接 | | 实现与已部署网络安全综合展示子系统的数据可视化展示融合，对智能分析预警平台分析的风险结果数据融合可视化展示。 |
| ▲网络安全管理核心平台接口对接 | | 实现同已部署网络安全管理核心平台业务处置流程对接，对智能分析预警平台分析的安全风险实现省、市、县流程处置和级联钉办功能。 |
| 网络安全管理APP接口对接 | | 实现与人社安全管理APP的数据接口对接，对智能分析预警平台分析的安全风险数据实现在APP上集中数据展示；省、市、县流程处置和级联钉办功能。 |
| 网络和通信安全分析 | 流量异常分析 | 通过智能学习算法实现对访问终端计算机的流量均值（包括上行、下行流量）画像，对超过均值区间的流量视为流量异常行为。 |
| 网络会话异常分析 | 制定终端通过进程和服务互相通信的安全连接机制：连接次数、连接持续时间的安全阈值（可根据网络情况和业务情况智能学习调整）。对黑名单进程和黑名单端口通信、超过安全阈值的连接行为视为风险连接。 |
| 网络边界安全分析 | 支持检测发现网络内存在的网络边界点，定位网络中存在的边界脆弱点；提供网络边界情况统计分析功能，针对NAT边界、网闸、上网代理、网络出口、无线ap，多网卡边界数据统计分析；提供网络边界详情列表和查询功能，包括：序号，边界类型，边界IP，运行状态，首次发现时间，最后发现时间，最后更新时间，子网情况/访问记录，边界详情。 |
| 访问控制安全分析 | 通过对终端系统日志信息、访问日志信息、网关流量日志信息的综合分析。实现对于未授权登录和访问受控区域内的终端和服务器信息，访问行为已触及安全访问基线的风险行为进行风险提示，并且关联其访问日志信息；对主机频繁发生内部访问和信息请求行为的风险提示。 |
| 数据使用安全分析 | 信息泄露 | 支持通过对网络、终端日志监控，对系统存在的敏感文件，移动介质拷贝、打印、刻录、邮件等过程当中存在敏感信息泄露的行为进行风险分析和监测。 |
| 应用异常访问 | 通过对终端应用访问数据和网关镜像流量数据的综合分析，实现对核心业务系统的应用访问异常监控，包括频繁访问异常行为、越权访问异常行为、下班访问行为、访问内容携带敏感数据，并且支持对异常访问行为的日志取证功能。 |
| 数据库异常访问 | 支持对数据库系统日志，数据库访问行为日志的数据采集。对违反数据库安全配置基线（包括口令、密码、访问控制等）进行风险提醒；对跨区域、越权等异常访问行为进行风险提示。 |
| 文件外泄轨迹流转 | | 针对内网终端发生含敏感关键字的文件外泄行为，进行溯源分析。根据md5值、文件操作日志和文件下载行为日志进行同一份文件的流转轨迹关联匹配，实现对泄露文件和数据的来源关联。  详细功能如下  1)实现对外泄文件的文件名，关键内容信息的提取。  2)实现对外泄文件轨迹画像，包括文件源头、移动过程、外泄出口记录。  3)支持对文件操作日志记录的信息检索。 |
| 全文日志检索 | | 通过对内网采集的流量日志数据和终端日志数据进行关联检索，展示出相关联的日志信息，辅助安全管理人员开展威胁行为深入分析。记录终端、网关、第三方采集的全量日志，提供对该日志的全字段自定义检索功能。 |
| 系统安全审计 | | 支持对自身系统的操作审计与日志记录功能。 |

* + - 1. 网络安全协调指挥指标要求

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| ▲兼容性 | 满足省委网信办“建成网络安全信息通报和事件应急响应指挥体系”的要求，按照《浙江省网络安全协调指挥平台建设指南》提升省人力社保厅网络安全协调指挥能力，建设内容包括实时监测、态势感知、信息通报三个功能模块。各业务系统模块流程机制须满足浙江省网络安全协调指挥平台建设指南中对业务流程的说明要求，须满足《浙江省网络安全协调指挥平台网络安全协调指挥能力平台建设指南》中对平台数据规范、平台数据接口的要求，并能与浙江省委网信办网络安全协调指挥平台实现对接。  要求能与省人力社保厅现有的网络安全管理核心平台实现无缝对接，报送相关风险事件数据。 |
| 数据收集 | 支持Syslog、FTP、https协议日志收集；  支持安全事件标准协议的数据；  支持多文件类型的复合数据；  支持动态配置模板来支持新的数据源； |
| 数据预处理 | 支持对各种来源日志进行归一化处理；  支持对各种来源日志进行IP详细信息，域名详细信息，单位信息等信息的补充完善；  支持对数据的不同形式描述进行标准化处理；  支持识别质量低下的数据并且归档记录；  支持对各种来源日志合并到最终统一数据流进行基础和高级分析；  支持多租户的数据空间隔离；  支持对各种来源安全事件自动智能转换到标准分类；  支持对相似日志的多种去重合并算法； |
| 基础分析能力 | 支持对全库数据的复杂条件查询；  支持对各种数据源多种维度的分布统计；  支持对各种数据源多种维度的时间轴统计；  支持对各种数据源多种维度的重要性聚合；  须具备数据库行为分析系统及分析方法或技术。 |
| 权限管理 | 角色分为超级管理员，管理员和用户三种权限；  超级管理员负责管理所有的用户和高级的维护功能；  管理员负责所有接口的维护功能；  用户可以按照需要细分到接口级别的权限； |
| 数据检索 | 须具备在大数据存储量中快速检索的方法或技术 |
| **实时监测** | |
| 总体要求 | 具备监测数据分析能力和安全威胁分析能力，汇聚监测对象所受的攻击威胁、破坏、窃密、渗透等威胁信息，以及该对象网络、系统、数据等安全隐患和漏洞信息等，为后续预警、通报、应急处置等工作机制流程提供数据支撑。 |
| 监测手段 | 对监测对象（资产）的监测手段包括可用性监测、脆弱性监测、敏感词监测、篡改监测，主要内容包括以下几个方面：  支持新增、修改监测对象（资产）时自动创建、修改各类监测任务；  支持自定义单条、批量设置各类监测任务状态及监测周期等策略；  支持对监测对象、监测地址、监测周期、监测任务是否开启等信息进行过滤搜索。 |
| 监测数据 | 支持获取监测对象（资产）的各类监测任务的结果，内容包括：  支持获取网站可用性、脆弱性、被篡改、敏感词监测结果。  支持网络资产数据、网站安全监测数据、流量监测数据、网站安全防护数据、第三方威胁情报数据预处理后的呈现和展示。 |
| **态势感知** | |
| 总体要求 | 基于平台获取的针对省人力社保WEB应用系统的各类监测数据及日常业务流转产生的业务数据，对网络空间安全相关信息进行汇聚融合及分析，从不同视角感知网络安全态势，分析结果形成态势感知模块的六大类态势感知应用包括综合态势、资产态势、威胁态势、网络攻击态势、事件态势、预警处置态势。 |
| 综合态势 | 支持网络安全总体态势分析，包括当前监管对象统计、实时监测隐患数统计、通报预警统计、风险趋势、高危系统排名、高危地区排名、监测对象分布统计、事件与隐患统计、通报预警统计等内容。 |
| 页面数据支持同时从不同时间维度筛选出数据作为展现，时间维度至少包含：近一周、近一个月、近三个月、近一年等； |
| 地图需支持全屏化展示，显示街道地图，便于重点时期对于网络安全事件应急处置进行指挥调度。且具备地域列表按钮，点击对应的地域，地图需支持跳转到对应地域的地图。 |
| 监管对象分类至少包含重点单位、重点系统、政务云系统、市直属系统、ICP备案和接入地市等几类。 |
| 实时监测隐患事件分类至少包含网站后门、DDOS攻击、僵木蠕病毒、入侵攻击、反共、黑页、博彩等类型。 |
| 风险趋势、高危系统排名、高危地区排名、监测对象分布、事件与隐患、通报预警统计等内容需支持查看详情。 |
| 资产态势 | 以资产对象为视角统计展示资产概况，包括资产基础信息以及资产相关安全类数据，内容包括：  1.支持对资产总数进行统计并可查看详情；  2.支持对资产类型的资产进行分类统计并可查看详情；  3.支持对资产重要等级进行分类统计；  4.支持对资产进行风险分析排名；  5.支持对资产存在漏洞数进行排名统计；  6.支持对资产受攻击次数进行排名统计；  7.支持对资产安全评分进行排名展示；  8.支持根据资产相关信息在地图上打点单位，且支持单位信息在地图上的轮播；  9.支持对资产的资产类型进行分类统计与资产重要等级分类统计的组合展示；  10.支持对资产各类分析的组合可视化展示。 |
| 威胁态势 | 威胁态势以安全漏洞为视角展示漏洞情况，漏洞数据源来自监测中心对资产中心资产的监测结果，内容包括：  1.支持根据单位/部门的漏洞信息在地图上打点，且支持相关信息的轮播；  2.支持对资产漏洞进行漏洞趋势分析；  3.支持资产漏洞数总数、漏洞类型分布、漏洞概况分布的统计；  4.支持漏洞影响单位/部门排名；  5.支持漏洞影响资产排名、漏洞影响URL排名；  6.支持展示最新漏洞信息等所有信息均支持查看详情；  7.支持对漏洞影响（影响单位、资产、URL）进行组合展示。 |
| 网络攻击 | 支持网络数据来源统计，支持网络攻击分类及统计、监控总览及分类、最新攻击消息、攻击趋势、受攻击行业分布、攻击类型分布、攻击区域/受攻击区域排名、攻击IP/受攻击IP排名、攻击源流量等。 |
| 监控总览需按不同协议类型数进行分类统计。 |
| 攻击趋势、受攻击行业分布、攻击区域/受攻击区域、攻击IP/受攻击IP需支持查看详情。 |
| 支持按时间（近一周、近一个月、近三个月、近一年）、攻击类型分布、攻击区域（境内攻击源/境外攻击源）、攻击IP/受攻击IP排名等内容进行筛选统计和展示。 |
| 安全事件 | 支持安全事件分析，内容需包含重点监测系统数、安全事件数、安全事件分类统计、事件趋势、最新事件概览、事件类型分布、事件区域排名、事件取证展示等。 |
| 安全事件分类需包含拒绝服务攻击、扫描探测、隐患利用、有害程序、信息篡改等其他类型 |
| 事件趋势、事件类型分布、事件区域排名需支持详情展示。 |
| 预警态势 | 支持预警态势分析，内容需包含一般预警数量统计、专项预警数量统计；  支持按时间、地域等维度展示预警等级分布、处置效率统计、预警列表、专项预警行业统计、专项预警区域分布、近一年预警统计等。 |
| **信息通报** | |
| 总体要求 | 支持对实时监测模块发现的安全隐患、漏洞等安全问题进行通报预警，本业务功能应至少包括以下子功能模块：通报综览、通报管理、签收回执、通报跟踪和安全问题展示。 |
| 通报综览 | 支持对通报情况的综合展示，展示的信息应包括以下内容：  支持展示发送通报情况，包括主送单位情况、抄送单位情况、影响资产情况、签收情况、回执等情况。  支持展示接收通报情况，包括发送方情况、问题处置期限、剩余时间、回执等情况。  支持对通报主送单位的统计、抄送单位的统计、签收情况的统计、回执情况的统计。 |
| 通报管理 | 通报管理包括以下几个方面:  支持通报发送方对通报信息的管理，如通报的新增、删除、查看、修改、撤回等基本管理操作；  支持对接入第三方数据源上报的网络安全问题进行通报；  支持新增、编辑通报时设置主送单位、抄送单位、影响资产、通报是否需回执、通报问题涉及的图片、文件等信息； |
| 通报签收回执 | 通报接收方可针对通报信息进行签收回执，主要内容包括：  1.支持通报接收方对通报情况进行签收，支持发送方查看整体签收情况及占比；  2.支持通报接收方对通报情况进行回执，回执内容包括对通报接收情况的描述、通报处理进度、涉及到的图片文件等信息。 |
| 通报跟踪 | 通报跟踪用于管理各安全问题的通报进度和处理进度，具体功能要求如下：  通报接收方可对通报进行跟踪，将通报情况的处理结果进行描述和回复，同步各类通报处理进度，并支持携带附件；  通报发送方可针对通报的签收和回执情况进行跟踪，支持查看签收占比、回执占比，支持下达催促接收方及时签收回执，并支持携带附件。 |
| 安全问题展示 | 针对安全类问题、安全事件、安全告警、日志、安全漏洞、敏感词、篡改信息进行综合展示：  支持对安全事件、安全告警进行综览和具体信息的组合展示，内容包括：威胁等级、起始时间、事件或告警名称、攻击意图、源IP、目的IP、攻击连、编号、结果分类、描述、处置建议、处理状态、处置结论、攻击意图、攻击策略、攻击方法、摘要内容、数据的采集解析内容、数据分析内容、原始内容、事件消息等；  支持针对日志进行综览和具体信息的组合展示，内容包括：采集器接收时间、设备IP地址、设备名称、源、目的、应用协议、目的端口、事件名称、问题来源信息、问题目的信息、报文信息、摘要信息、原始日志、以及其他更多内容；  支持整体展示所有资产漏洞监测结果，支持根据漏洞威胁等级对漏洞进行分类展示，展示漏洞相关信息包括漏洞名称、漏洞级别、漏洞编号、漏洞描述、漏洞修复建议、影响资产列表、漏洞位置、漏洞内容等；  支持整体展示所有Web资产敏感词监测结果，并根据敏感词分类展示敏感词监测结果的具体内容，包括敏感词、事发URL、事发URL敏感词位置、源码定位、快照定位等信息；  支持整体展示所有Web资产被篡改结果，展示内容包括篡改数量、被篡改URL、篡改片段、篡改前后源码对比以及快照定位等信息。 |

3.1网络安全协调指挥-主动监测专用设备指标要求

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 产品规格 | 硬件规格：2U，内存：≥32G，硬盘：≥2T\*1，网口：千兆RJ45网口≥2，电源：1+1冗余电源 |
| 产品性能 | 单系统支持扫描不少于80个网站数 |
| 7\*24自动监测 | 支持7\*24小时自动监测服务、实现对网站漏洞监测、网页木马监测、敏感内容、可用性实时监测； |
| 平台支持周期性、单次与指定时间的监测； |
| ▲API接口 | 系统数据接口须符合《浙江省网络安全协调指挥平台建设指南（2018版）》中对安全隐患数据接口的要求。须能实现与本次建设的网络安全协调指挥系统对接，为平台提供基础网站安全监测隐患数据。 |
| 支持协议 | 支持http、https、wap协议；  支持web2.0解析、Flash解析； |
| 支持包括Basic、Digest、NTLM在内的认证方式； |
| 代理模式 | 支持HTTP和SOCKS代理，并支持相应代理的认证方式； |
| 监测策略 | 支持漏洞扫描、网马监测、敏感关键字监测、可用性监测的独立策略设置，可独立配置监测周期、监测深度、监测页面数、监测引擎的独立指定； |
| 支持策略的灵活配置，可配置网站中扫描页面黑白名单，爬行名单等，支持在权限较高的管理后台中监测；  支持限制扫描引擎的最大并发连接数，防止对网站产生过大访问压力 |
| 支持在指定扫描时段的扫描，非允许时段会自动暂停扫描任务。 |
| 须具备基于JAVA的网页动态安全漏洞检测方法或技术 |
| 漏洞扫描 | 须支持网页漏洞扫描，扫描SQL注入、XSS跨站脚本、伪造跨站点请求（CSRF）、网页木马、隐藏字段、表单绕过、AJAX注入、弱配置、敏感信息泄漏、弱口令、Xpath注入、LDAP注入、框架注入、操作系统命令注入、Flash源代码泄漏、Flash跨域攻击、Cookie注入、敏感文件、第三方软件、其他各类CGI漏洞等各种类型； |
| 须支持漏洞风险跟踪视图，进行历史风险跟踪与比对； |
| 支持对注入类漏洞进行渗透功能，能实现提取数据库类型、名称、表与字段等数据 |
| 支持对漏洞进行自定义检测功能，支持修改测试请求再次检测； |
| 支持对漏洞检测过程展现与分析，可比对正常请求与检测攻击的区别； |
| 系统须支持提供漏洞验证功能； |
| 须提供漏洞修复建议自定义功能，提供单独的漏洞提供建议。 |
| 须支持漏洞结果人员审核功能，可删除、增加漏洞记录 |
| 可用性监测 | 支持对网站的应用可用性监测，访问延时监测，能及时识别网站的应用异常； |
| 支持对网站域名安全监测，及时识别域名解析变更，解析域名所在地，可检测域名劫持并告警； |
| 支持可用性异常告警，可配置异常超过多长时间即进行告警； |
| 网马监测 | 支持多种挂马方式检测，如：Iframe、CSS、JS、SWF等；  须具备针对Javascript恶意代码的智能检测方法或技术 |
| 外链监测 | 支持检测页面中的可疑外链；  支持检测页面中的错链、坏链； |
| 敏感关键字监测 | 支持定义关键字内容与分组； |
| 支持各种语义分析识别关键字； |
| 系统引擎调度要求 | 支持实现引擎智能调度，可将任务负载均衡分配至饱和度较低的引擎。  任务下发前调用引擎进行扫描目标访问速度确认，择优下发至负荷小且速度快的引擎。 |

3.2网络安全协调指挥-威胁感知业务探针指标要求

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 产品规格要求 | 2U标准机架式设备；配备1+1冗余电源； |
| 磁盘空间≥1T，支持硬盘RAID1； |
| 管理口：≥2个千兆电业务口；  业务口：≥4个千兆电业务口 |
| 产品性能要求 | 网络层：2Gbps，应用层：1Gbps，WEB检测：HTTP最大并发数7万/秒，邮件检测：邮件处理数: 150万封/24小时，文件检测：5万个/24小时 |
| 部署方式 | 旁路模式部署 |
| ▲API接口 | 系统数据接口须符合《浙江省网络安全协调指挥平台建设指南（2018版）》中对网络攻击事件数据接口的要求。须能实现与本次建设的网络安全协调指挥系统对接，为平台提供基础WEB攻击、Mail攻击、文件攻击威胁事件数据。 |
| 审计协议 | 支持审计http、ftp、smtp、pop3、smb、imap等协议报文；  支持Mysql/MSSQL/DB2/Oracle等协议报文；  支持LDAP登录行为的识别；  提供审计协议类型的端口号配置，可根据需要变更端口号； |
| 检测风险类别 | 支持检测WEB攻击、异常访问、恶意文件攻击、远程控制、WEB后门访问、发件人欺骗、邮件头欺骗、邮件钓鱼、邮件恶意链接、DGA域名请求、SMB远程溢出攻击、WEB行为分析、隐蔽信道通信、暴力破解（包括SSH、TELNET、RDP、FTP暴力破解）、挖矿等风险 |
| 弱口令风险检测 | 支持对Telnet、FTP、POP3、SMTP、IMAP等协议进行弱口令检测 |
| 告警详细展现 | 支持详细展现告警级别、时间、威胁名称、状态、客户端IP、客户端IP所在地理位置、服务端IP、服务端IP所在地理位置、报文、操作等信息，包含请求URL、请求类型、请求内容、请求头、Host、User-Agent、Accept、Accept-Language、Accept-Encoding、Accept-Charset、Keep-Alive、Connection、Cookie、请求参数、响应码、返回长度等信息； |
| 主机威胁分析 | 支持自动对内网主机进行威胁指数分析，详细展示具体的威胁指数、威胁活动、历史威胁指数、遭受的攻击类型、攻击次数、攻击状态等； |
| 支持根据不同威胁指数的主机实现攻击溯源和攻击过程的可视化分析； |
| 支持通过攻击源、攻击目的对攻击路线进行统计，包括攻击的行为、告警，并以直观的图形化形式展示； |
| 木马回连分析 | 支持自动学习网络流量中包含的各种可疑C&C IP/URL，包含各种可能对内网存在影响的IP和域名； |
| 支持快速识别网络中存在的恶意回连行为，包含回连主机IP、服务器IP、时间、行为等； |
| 支持对基于木马回连的非法数据传输等行为进行取证分析，包括回连主机IP、服务器IP、传输数据大小、协议类型等； |
| 解析协议 | 支持HTTP协议、webmail、SMTP、POP3类型报文解析；WEB攻击检测；  支持HTTP、FTP、SMB、SMTP、POP3等协议传输文件检测； |
| 双向审计 | 支持双向审计，对请求和响应都进行审计； |
| 攻击检测 | 支持SQL注入、命令注入、跨站脚本、代码注入、协议错误攻击检测； |
| WEBSHELL检测 | 支持WEBSHELL检测，可检测访问webshell的行为，包含具体对应的URL、返回码、返回数据包内容等； |
| 自定义WEB审计规则 | 支持根据来源IP、MAC、HTTP请求方法、URL、请求头、请求参数、响应码等内容设置审计规则高、中、低等风险等级； |
| 动态分析 | 支持自动关联行为分析的详细展现，包含SQL注入取数据、表单破解、XSS测试、目录穿越读取文件、多人访问Webshell、APT攻击等； |
| 场景化分析 | 支持场景化的分析能力，对发现的告警进行二次关联，支持对勒索病毒、网站后门、邮件APT攻击等事件进行预警； |
| DNS协议分析 | 支持具备DNS协议分析能力，发现受感染主机、危害程度、被感染病毒类型、回连C&C域名、DNS返回详情、恶意主机明细等行为。 |
| Webmail攻击检测 | 支持基于webmail攻击类型检测，包括sql注入、跨站、命令注入等攻击检测； |
| 社工类攻击检测 | 对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接； |
| 恶意附件检测 | 支持邮件恶意附件行为检测； |
| 文件类型 | 支持doc, xls, ppt, swf, pdf, java, rar, zip, rar, exe, vbs, scr, html，js等多种文件解析； |
| 自定义文件类型 | 支持添加或删除指定审计文件类型； |
| 特征检测 | 对文件进行特征匹配，利用已知的特征库发现恶意可以执行代码；  对文件进行特征匹配，利用已知的特征库发现恶意的非可执行文件； |
| Shellcode检测 | 支持通过分析文件中的二进制代码，找到文件溢出攻击的代码，并能找到APT攻击中的0day攻击； |
| 动态沙箱检测要求  子文件扫描  攻击样本提取 | 支持对存在问题的文件输出完整的二进制动态分析报告；  动态执行可疑文件，分析代码的注册表、进程、网络、文件等行为，分析其安全风险；  需支持对文件关键行为进行截图能力；  可展示文件中版本信息、段信息、资源信息、导入表、字符串信息、删除文件信息等内容；  可展示ROP行为检测；  可展示具体文件的行为，包括所有的注册表行为、进程行为、互斥量、进程运行的函数、返回结果、返回值等信息； |
| 对文件内部嵌入的子文件可进行二次扫描，分析安全性； |
| 支持提取出攻击的完整样本文件，并提供对该文件下载的能力； |
| 威胁态势指数 | 支持展示威胁程度最高的文件样本MD5、威胁指数、传播次数，病毒检测、静态检测和动态检测结果等内容； |
| 支持根据文件传播情况分析受感染主机、接受云端威胁情报、关键威胁行为可视化、回连主机host和完整沙箱分析报告； |
| 支持根据云端威胁情报展示云端是否确认、传播协议类型、传播次数、云端确认结果等； |
| 支持自动备份审计日志，备份完后通过FTP方式外送到外部设备；  备份文件需要进行加密，且必须导入设备才能够进行恢复查看； |
| 当磁盘空间达到一定的阀值，支持自动清理最早的数据释放空间。 |

4.服务器安全加固指标要求

|  |  |  |
| --- | --- | --- |
| **指标项** | | **指标要求** |
| 总体要求 | | 服务器安全加固扩容，根据人社业务系统资产数量增加授权数，为服务器提供外设管控、文件审计、违规外联检测与阻断等主机安全加固防护。要求能与省人力社保厅现有的网络安全管理核心平台实现无缝对接，报送相关风险事件数据。 |
| 产品描述 | 自主知识产权 | 软件要求在中华人民共和国境内开发，具备自主知识产权。 |
| 易用性 | 软件界面友好，易于安装、配置和管理，并有详尽的技术文档。软件图形界面以及各类技术文档均为中文。 |
| 节点数量 | 扩容支持250个服务器节点。 |
| 支持的终端环境 | 支持的操作系统 | Windows server 2003、Windows server 2008、Windows server 2012、Windows server 2016、win xp 、win 7、win 8、win 10、Centos 5.0 +、Redhat 5.0 + 、Suse11 +、Ubuntu 14 +、华为泰山、中标麒麟、银河麒麟、凝思等操作系统。 |
| Web服务器 | Apache 2.0-2.4、IIS6、IIS7、IIS8、IIS10、Java系列(JBoss、Tomcat、Weblogic、Websphere)等。 |
| 数据库 | MSSQL，Oracle、Sybase、Informix、DB2、MySQL等关系型数据库；Mongodb、Cassandra等非关系型数据库。 |
| 核心功能 | 系统性能监控 | 支持对CPU使用率监控、内存占用率监控、磁盘读写监控、上下行流量监控，在达到配置阈值时报警。 |
| 支持网络通信全时监控。 |
| 系统安全性模块 | 支持防端口扫描，防违规外联，锁定恶意的端口扫描及外联行为，并记录告警。 |
| 违规外联支持黑、白名单双模式，白名单模式可配置是否允许访问特定的网站和地址；黑名单模式可自定义恶意IP，支持黑名单告警和阻断。 |
| 支持反渗透监控，包括横向渗透的危险操作等。 |
| 支持网站防护，包括SQL注入、XSS、Web应用及容器漏洞防护、访问控制、屏蔽扫描器等。 |
| 支持智能检测防御CC攻击，并可进行高、中、低三档设置。 |
| 内核级防火墙（业务间流量东西向隔离）功能，包括IP、端口、协议、流向等细粒度权限控制。 |
| 支持流量画像，支持全网流量可视化、应用级流量可视化；支持威胁横向扩散路径可视化与一键阻断；支持违规外联路径可视化与一键阻断。（提供产品功能相关证明材料） |
| 支持登录防护，包括以系统账号为粒度的异常登录防护、支持五个任意维度(任意地理位置，任意IP，任意域名，任意计算机名，任意时间)的系统登录访问策略设置、防暴力破解、弱口令检测并告警。触发登录防护后，自动联动添加微隔离规则。 |
| 支持显示隐藏的系统账户。 |
| 具有系统漏洞扫描和修复功能，提供真实漏洞补丁。管理中心可作为补丁服务器，支持管理中心可上网和不可上网2种情况。提供离线补丁下载器，按需智能获取内网所需补丁。 |
| 支持对文件变化的审计。 |
| 支持对移动存储设备的行为监控、权限管理、行为审计。 |
| 支持对无线网卡的使用审计、权限管理 |
| 支持用户录制定制化的配置模板，应用到所有或者指定的机器上；自带10个以上默认模板。对关键操作，比如病毒查杀等关键安全项检查支持创建自动巡检任务，定时执行。 |
| 支持开启进程黑名单，阻止不受信任的程序启动和生成，同时支持路径和MD5两种形式。 |
| 支持开启进程白名单，只允许受信任的进程启动，同时支持路径和MD5两种形式。 |
| 防病毒模块 | 支持文件实时监控，在进程启动、文件创建、存储介质连接时自动触发。 |
| 可保护系统指定文件不被恶意篡改或执行。 |
| 可防止指定命令被恶意利用，损害主机。 |
| 支持对顽固流行病毒进行智能拦截。 |
| 支持域环境下普通账户登录的病毒木马查杀及策略的配置。 |
| 开启进程监控后能完全预防已知病毒的危害。 |
| 提供专门的勒索风险评估功能。至少需要包含：弱口令检测、系统漏洞检测、恶意进程检测、高危端口检测等能力。 |
| 提供专门的针对已知勒索病毒的防御引擎，并提供功能开关项。对于已知勒索病毒确保进程无法启动。 |
| 提供专门的针对未知勒索病毒的防御引擎，并提供功能开关项。对于未知勒索病毒确保无法加密。支持白名单设置。 |
| 提供专门的挖矿风险评估工具。评估项目至少包括：弱口令、系统漏洞、恶意进程、DNS历史查询、违规外联等。 |
| 提供专门的挖矿实时防御工具，并提供功能开关。 |
| 自研免疫引擎通过强制访问控制技术免疫WannaMine1.0/2.0/3.0等免杀病毒 |
| 支持强力查杀，对于无法普通隔离的病毒文件强制停止进程并隔离或动态移除到删除队列。 |
| 支持部分病毒感染文件的修复功能，对于二进制文件可剥离感染部分，保证应用正常使用 |
| 支持查杀映像劫持类型的病毒。 |
| 支持查杀防范网页中的恶意代码。 |
| 支持对压缩文件、打包文件查、杀毒（默认支持9层压缩扫描，可根据用户需求增加扫描层数）。 |
| 支持运行文件查杀毒。 |
| 支持支持图片、视频等多媒体文件的查杀毒。 |
| 支持查杀各类Office文档中的宏病毒、夹带型木马。 |
| 支持在线、离线病毒库升级。 |
| 支撑功能 | 情报云脑 | 支持对恶意文件进行自动化动静态分析，获取样本行为分析、样本同源性等分析。支持IP&域名&文件&邮箱的信誉判断，可以对应急响应事件进行处置溯源分析，还可以获取可视化数据形成黑客团伙画像及获取实时的热门威胁情报。 |
| 文件推送 | 支持下发文件、安装应用程序、远程执行命令 |
| 屏幕水印 | 支持对屏幕拍照泄密数据的行为进行溯源。 |
| 告警功能 | 告警类型包括：异常文件、网站防护、性能监控、登录防护。 |
| 告警内容至少包括事件发生时间、事件类型、访问的资源、 IP源地址等详细内容。 |
| 告警方式包括：Email，短信，syslog，snmptrap，自定义。 |
| 升级系统 | 支持离线升级及在线自动升级，包括管理中心平台、客户端程序、病毒库、补丁库、Web后门库、违规外联黑名单库。 |
| 客户端程序支持在线热升级，升级之后旧版本驱动等程序无残留。 |
| 管理功能 | 集中管控 | 管理平台支持一键卸载客户端、一键设置客户端卸载密码、一键停止/恢复所有防护、一键解除绑定。 |
| 支持导出已安装客户端程序的资产清单。支持导出日志。 |
| 能够通过统一的管理中心对多个服务器或主机进行监控。 |
| 能实时检测工作组件工作状态以及系统关键资源的运行状态。 |
| 能对服务器或主机节点进行分组管理。 |
| 支持多级中心部署，查看所有下级控制中心的资产部署情况以及风险数据。 |
| 用户管理 | 支持多级用户管理：系统管理员、租户管理员。 |
| 至少支持以下帐号管理功能：帐号创建、帐号授权、帐号属性修改和帐号删除。 |
| 进行身份认证，用户切换角色时，必须进行重新认证。 |
| 支持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。 |
| 管理界面 | 支持SSL的Web界面。 |
| 许可到期前提醒。 |
| 可视化功能 | 能展示各个服务器或主机节点的信息，运行状态、活动规律、行为变化趋势和详细资料，以及历史行为数据查询、全局安全态势等。 |
| 能监测节点遭受网络攻击的趋势信息，可以直观的了解攻击目标、攻击源、攻击方式的变化趋势和详细资料。 |

5.漏洞风险监测指标要求

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 整体要求 | 标准机架式，CPU配置≥8核，内存配置≥16G，硬盘配置：≥1TB，接口：≥2千兆网卡，冗余电源。  对资产漏洞风险监测，漏洞扫描、弱口令扫描、网站安全漏洞扫描、漏洞自动化巡检、基线检测，3000资产授权。 |
| 漏洞检测 | 漏洞检测方式：采用高精度检测脚本，漏报率极低，高危漏洞漏报率不高于1%。 |
| 系统漏洞库能够覆盖了常见的操作系统漏洞、软件漏洞、最新的网站框架应用漏洞等。能够针对操作系统以及web漏洞进行检测。 |
| 漏洞类型兼容：CWE  漏洞库兼容：CNVD、CVE、CNNVD |
| 基础漏洞检测：支持常见CMS应用漏洞，支持常见第三方框架和组件近8年高危漏洞和部分中低危漏洞，运维类漏洞如敏感文件泄露，目录穿越等漏洞的扫描。 |
| 主机合规检测：基于服务版本对主机资产进行合规检测。 |
| 弱口令检测：支持MySQL,SSH,FTP,SQLServer,Redis等常见服务的弱口令扫描，支持弱口令字典自定义。 |
| 网站WEB漏扫：支持按照URL地址、周期、设置监控选项、并进行cookies、配出页面、爬虫深度、爬取URL数、扫描频率的设定进行扫描，支持SQL注入，XSS跨站脚本，命令执行等30多种常见通用漏洞类型扫描，包括1500+通用漏洞规则。 |
| 支持主机漏洞检测，不少于35类。 |
| 网站内容检测：支持违规内容检测（涉黄/涉赌/涉政/虚假证件）、篡改检测，准确率高达97%。 |
| 基线检测：支持禁止端口及服务开放基线设定，确认是否已开放。 |
| 漏洞管理 | 支持漏洞检测频率设置，可自定义扫描周期及检测时间。 |
| 支持漏洞自动复测间设置（关闭、自定义开始时间点）。 |
| 支持漏洞信息检索功能，可快速定位不同漏洞类型，不同资产漏洞。 |
| 支持通过资产指纹进行漏洞分析，并从资产的类型、服务版本、漏洞类、漏洞严重程度等多个维度进行关联保存。 |
| 支持按照漏洞名称、地址、资产IP、资产域名、漏洞状态、处理状态、发现时间进行展示。 |
| 支持漏洞查看、重新检测、漏洞处理。 |
| 支持漏洞一键导出Excel查看、一键分享给相关人员查看 |
| 支持漏洞确认、忽略操作。 |
| 自定义检测 | 支持资产自定义更新检测：对资产临时检测，观察资产变动情况（检测结果包括主机更新数、网站更新数）。 |
| 支持风险自定义检测：对资产临时进行风险检测，检测内容包括应急插件、基础风险检测、WEB风险检测，检测结果包括漏洞风险数、合规风险数。 |
| 支持应急检测，能够有针对性对单、多个指定的漏洞进行指定范围的检测，快速精准定位。 |
| 支持网站可用性监控、主机可用性监控。 |
| 系统管理 | 支持漏洞告警（站内信、邮件、短信）。 |
| 支持日报定时推送：掌握资产分布状况以及风险态势。 |
| 支持在线升级、离线升级（包括系统版本更新和漏洞库更新）。 |
| 严重高危漏洞48小时内可出检测插件以及修补补丁，常规普通漏洞两周内更新一次。 |
| 支持对账号信息进行管理，包含账户名称、注册邮箱、联系手机、密码强度、企业名称、所属行业。 |
| 支持资产报表、漏洞风险报表生成，支持在线查看，并以Word ,Excel形式导出。 |
| 支持白名单添加，对白名单资产不进行漏洞巡检检测。 |
| 支持二层账号体系：超级管理员&普通用户，支持多账号体系的运营管理，包括全局的账号管理，资产管理，漏洞命中分析等功能。 |
| 超级管理员：查看用户的资产/风险情况，创建风险扫描规则，管理用户添加/删除/编辑等。 |
| API开放 | 支持API接口开放，可通过API接口实现创建扫描任务、获取扫描任务进度、启停扫描任务等动作。 |
| 部署方式 | 设备支持单台、多台、分布式、云上部署模式。 |
| 对接接口 | 实现安全智能分析预警安全数据接口对接,提供安全漏洞数据到安全智能分析预警，为内部安全事件管理提供有效分析处理数据。 |

6.数据库防护系统指标要求

|  |  |  |
| --- | --- | --- |
| **指标项** | | **指标要求** |
| 总体要求 | | 数据库安全防护扩容，在内网服务器区域增加数据库防护系统授权，对重要数据库操作行为进行安全审计记录和安全防护。要求能与省人力社保厅现有的网络安全管理核心平台实现无缝对接，报送相关风险事件数据。 |
| ▲配置 | | 至少支持3个系统的数据库防护部署，不少于6个数据库实例安全管理。 |
| 数据库支持 | | 至少需支持包括ORACLE（单机及RAC）、MYSQL、SQLSERVER、DB2、GBASE8.3S等主流数据库系统。 |
| 准入 控制 | 多因素 准入控制 | 支持多维身份管理，至少包括应用程序名、IP地址、主机名、操作系统账户、数据库账户、数据库实例名、时间、U盾等因素进行任意组合，并可以组合形成新的登陆认证规则。 |
| 支持对SQLPLUS、PLSQLDEV等SQL管理工具进行签名登陆验证，防止工具程序随意连接数据库。 |
| 应用 防假冒 | 支持对假冒应用识别和拦截，防止假冒应用访问数据库。 |
| Ukey登录 | 支持Ukey及软证书等方式进行证书登陆验证，从而对自然人进行识别和控制，可以为相关人员分为唯一的数字证书，实现对自然人的唯一验证，实现登陆过程不可抵赖。 |
| 防撞库  (密码泄露防护) | 支持检测和审计密码猜测行为，通过设置密码输入错误次数限制进行防护。达到密码输入错误次数，自动锁定攻击终端，支持自动解锁和手工解锁。 |
| 在数据库用户密码被泄露的情形下，仍能阻止非法用户登陆目标数据库，解决仅依靠密码认证带来的安全不足问题。 |
| 免密登录 | 支持免密登录功能，当数据库管理人员需要登录数据库时，无需输入数据库用户名密码，避免数据库用户和密码泄露。 |
| 访问 控制 | 特权账户管理 | 支持特权用户访问控制（如：DBA\SYSDBA\Schema User\any权限等用户），实现特权用户三权分立管理，满足等级保护等法规对安全管理的要求。 |
| 敏感数据访问控制 | 针对敏感数据集合的访问，需要要经过授权，不具备访问权限的操作，明确阻断拒绝，并提示“安全权限不足错误”。 |
| 敏感数据支持设置访问规则，访问规则中可设定精细化的访问因子（如应用程序名、IP地址、主机名、操作系统账户、数据库账户、数据库实例名、时间、U盾等条件），满足规则条件方可访问敏感数据。 |
| 支持限制特定的过程、函数、包等对象访问敏感数据。 |
| 可设置敏感标签身份，自动具备合法访问敏感数据的权限。未明确注册的身份，默认表示为不合法身份，不能访问敏感表格。 |
| 行数阈值管控 | 支持访问返回行数控制，对批量下载、更新等操作的控制，避免海量数据泄漏。 |
| 访问频次控制 | 支持访问频次控制，避免一定时间内的高批次访问，避免非法人员通过高频访问快速窃取业务数据。 |
| 敏感SQL管理 | 具有敏感SQL特征库，能够对勒索等恶意代码进行快速识别和防御。 |
| 危险操作控制 | 对于危险操作，如：Create user、Alter user、drop user等，授权管理操作(Grant)，业务对象操作（Truncat table，drop table）等操作，必须经过授权才能执行，防止人为误操作。 |
| 分级 分类 | 敏感数据分类 | 支持对敏感数据进行客体标签化定义，同时支持自然人、数据库用户、企业身份等访问主体的标签化定义，主体和客体通过敏感标签实现访问控制。 |
| 支持自定义敏感数据范围，可在表级和列级两个粒度进行配置，多个数据表格归类成为敏感数据集合，进行独立安全管理。 |
| 特权分类 | 预定义特权命令分类，支持对各类高危命令进行授权，只允许被授权的身份访问。 |
| 动态  脱敏 | 运维脱敏 | 支持SQLPLUS、PLSQLDEV等SQL管理工具查询数据时的动态脱敏，根据用户的身份与访问的数据库对象以及对应的脱敏规则，对不同授权的用户可返回真实数据、部分遮盖、全部遮盖以及其他脱敏算法得到的结果。  脱敏规则需要支持以下脱敏算法：  1、放行：对于已授权用户，返回真实数据；  2、返回空：对含有敏感表格或敏感列的数据结果返回为空值；  3、遮盖：全遮盖：默认以遮盖符‘\*’替换敏感列的值；  4、部分遮盖：对敏感列的值进行分段，替换其中的一段或数段值；  5、随机映射：对数值、字符或字符串进行随机映射处理。 |
| 工单 管理 | 运维安全管理 | 通过工作流的方式对表格和SQL访问授权，使整个过程更加透明，有迹可寻。简化安全管理流程，使安全管理更加便捷。 |
| 审计 | 运维审计 | 支持SQL命令的细粒度审计和分析，并详细记录管理用户的行为信息，包括该语句执行的时间、机器名、用户名、IP地址、MAC地址、客户端程序名以及SQL语句等信息，对数据库操作进行审计，可对查询，新增，修改，删除等行为进行监控。 |
| 审计管理 | 支持以搜索引擎条的方式进行搜索，提供类似于百度，谷歌的搜索方式；提供高级搜索，进行精确匹配搜索。 |
| 审阅 | 提供自动审阅，自动审阅过的审计信息，再次出现将不需要再行审阅，依赖于审计信息可以提取访问规则，把规则加入至访问及订阅规则库。 |
| 审计分析 | 提供一致性回溯分析、相同事件查看分析；并提供依赖于审计信息的即时报表分析。 |
| 告警通知 | 安全告警支持基于任意组合订阅的模式，实现个性化告警订阅管理。支持多种安全响应措施，包括页面、邮件、短信方式进行告警。 |
| 运行 模式 | 多模式 运行 | 支持学习模式、激活模式和模拟模式等多种模式。学习模式运行，支持SQL的自学习，识别安全SQL；模拟模式运行，可以提升安全策略准确性，避免对生产库的影响。 |
| 模式切换 | 在学习一定周期后，系统自动转激活运行，避免人工操作，简单快捷。 |
| 产品 部署 | 部署模式 | 支持透明代理和反向代理等模式部署。 |
| 支持 主备模式 | 支持当安全设备因宕机、系统本身主程序不可用、内存持续被占等问题导致不可用时，自动切换到另外一台安全设备进行运行。 |
| 支BYPASS 容灾功能 | 支持当安全设备全部不可用时，自动启用BYPASS功能，避免因安全设备本身影响业务系统。 |
| 风险 感知 | 风险监控 | 支持直观、可视化监控单位整体安全情况，当出现风险时可快速的定位当前被攻击的数据库及发起攻击的客户端。 |
| 24小时 监控 | 支持注入攻击监控、漏洞攻击监控、敏感访问监控、系统运行监控、流量监控等多角度展现近期攻击风险。 |
| 报表 | | 具有丰富的报表模板，报表可导出（包括：PDF、HTML、EXCEL、word等）。 |
| 平台 安全 | 三权分立 | 具有强大的自身安全机制，支持平台用户三权分立，可以系统管理员、审计员和保密员等不同的安全角色。 |
| 复杂口令 | 支持复杂口令配置。 |
| 白名单 登录 | 支持IP地址等要素作为验证机制，实现白名单登陆管理。 |
| 对接接口 | | 实现安全智能分析预警安全数据接口对接,提供安全事件数据到安全智能分析预警，为内部安全事件管理提供有效分析数据。 |

7.防火墙指标要求

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 配置要求 | 千兆电口≥10，千兆光口≥8，10G接口≥6，SSL VPN并发数实配100可扩展1000，IPSec VPN隧道≥10000，配置双电源；支持USB2.0；配置≥500G固态硬盘；配置3年IPS-AV-URL特征库升级；万兆多模模块≥6个，千兆光口多模模块≥6个。 |
| 性能要求 | 吞吐量≥25Gbps，最大并发连接数≥600万，每秒新建连接数≥25万，IPSec吞吐量≥4Gbps，IPS、AV开启后吞吐量≥10Gbps。 |
| 策略管控 | 能够基于IP、IPv6、MAC地址、时间进行访问控制策略控制;支持自定义安全策略，安全策略组功能；支持策略冗余/命中分析； |
| 路由功能 | 支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议。 |
| IPV6 | 支持IPv6协议栈、IPV6穿越技术、IPV6路由协议。 |
| 协议识别 | 可识别应用层协议数量≥1000种。 |
| 流量控制 | 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等；支持基于用户，IP的带宽保证；支持每IP，每用户的最大连接数限制，防护服务器；支持用户流量配额管理；支持流量整形； |
| 安全防护 | 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；  可以支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护；  支持对HTTPS，POP3S，SMTPS,IMAPS加密流量代理解密后，并进行内容过滤，审计，安全防护； |
| 可靠性 | 支持BFD链路检测，支持BFD与VRRP联动实现双机快速切换，支持BFD与OSPF联动实现双机快速切换。 |
| 智能DNS | 支持智能DNS功能、透明DNS功能、动态DNS功能，支持会话保持，满足多链路出口场景下的负载均衡，且该功能是免费的。 |

8.上网行为管理系统指标要求

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 硬件规格 | 最大并发连接数为100万，最大新建连接数为20000个/秒；  硬件规格≥2U，标配千兆电接口≥6个（其中含1个管理接口和1个HA接口），千兆光口≥2个（含2个光模块），扩展槽≥1个，硬盘存储≥1T，双电源。 |
| 设备必须提供物理硬件bypass按钮，便于设备巡检、设备故障时管理员无需重启、关机、断电即可恢复网络通畅。 |
| 支持远程登录在界面实现Bypass，并可进行切换。 |
| 采用国际先进的多核处理器硬件架构及多核并行处理系统。 |
| 部署模式 | 网关模式、镜像模式、网桥模式、Portal模式 |
| IPv6支持 | 能够支持IPv6环境下的网址访问审计、生成分析报表等功能；能够在IPv6环境下，正确审计显示用户的IPv6地址 |
| 常用应用软件控制 | 需要识别互联网上的绝大多数网页和应用，并对这些网页和应用进行管控.  应用协议库包含的应用数量不低于7100种，应用规则总数不低于30000种。  设备内置常用应用标签，分类至少包含内容外发风险、期货行业合规、证券行业合规、高安全风险、影响工作效率、消耗带宽6大类。  支持设置在设定时间段内禁止浏览无关网页和使用无关应用。 |
| 阻止内部敏感信息外发 | 需要识别互联网上的各种网页、应用，并能针对这些网页、应用进行互联网传输管控，不同网页被阻塞后会跳转不同的阻塞页面，有效避免内部人员通过互联网泄露机密文件；  同时，也对内部人员互联网言论进行关键字匹配过滤，可根据网页内容关键字进行审计与过滤，一条策略实现阻断、记录、告警，每个关键字对象要求可至少录入500个关键字，支持用户完全自定义，避免内部人员在互联网发表违法不良言论，降低单位因互联网使用不当带来的法律风险。  根据关键字管理搜索引擎访问；一条策略实现搜索关键字的阻断、记录、告警，方便维护。 |
| 防止私接路由 | 可识别网络中的私接路由的网络行为并配置阻塞策略 阻塞条件支持基于终端总数量、PC数量、移动终端数量分别配置 支持自定义阻塞时间 支持可配置阻塞IP或阻塞用户 支持单独配置是否阻塞非80端口流量 支持自定义阻塞页面内容，可上传图片或文件共阻塞页面使用。 支持基于用户或IP自定义免阻塞白名单 |
| 互联网上网行为记录 | 需要记录内部员工的上网动作，包括内容、发生时间等，并且需要长期保存以及可以对上网动作进行快速查询；  当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；管理员可查看用户反馈的分类错误，并可以选择向服务器反馈。 |
| 非法Wi-Fi热点管控 | 可识别网络中的非法接入wifi的网络行为并配置阻塞策略 阻塞条件支持基于终端总数量、PC数量、移动终端数量分别配置 支持自定义阻塞时间 支持可配置阻塞IP或阻塞用户 支持单独配置是否阻塞非80端口流量 支持自定义阻塞页面内容，可上传图片或文件共阻塞页面使用。 支持基于用户或IP自定义免阻塞白名单 |
| 首页行为风险面板 | 可集中呈现上网行为风险等级和状态；行为风险等级包括安全等级、效率等级、合规等级和管控等级；行为状态包括管控效果、运行状态、安全状态、泄密风险状态、合规状态和应用使用状态；点击页面数值可直接跳转查询详情。 |
| 病毒查杀 | 支持基于云端大数据安全平台，对恶意URL访问进行封堵和记录日志。 支持恶意URL访问日志查询，日志应包含时间/用户/终端类型/内外网IP地址和端口号/MAC/网址/网站类型/访问控制类型。 |
| 支持失陷主机检测 | 支持与威胁情报大数据平台对接，能够快速识别、封堵失陷主机、记录日志。 |
| 支持通过恶意软件特征检测方式识别失陷主机并记录日志 |
| 至少支持拦截对外部威胁IP的访问请求和阻塞失陷主机IP两种控制策略。阻塞后支持向用户推送威胁情报阻塞提示页面。 |
| 文件审计 | 支持对Windows百度网盘客户端的文件标题和内容审计 |
| 支持对QQ、微信和百度网盘的PC客户端外发文件进行关键字过滤和封堵 |
| IM审计 | 可针对QQ账号制定策略，对聊天、登录及登出的行为进行记录与控制；支持对QQ聊天内容进行审计。可制定多条QQ审计控制策略，实现针对不同的用户匹配不同审计策略 |
| 数据库审计控制 | 可审计、控制Oracle, MySql, SqlServer, PostgreSQL等数据库的访问与操作，包括添加、删除、修改、查询等。 |
| 二维码认证 | 支持接待人员扫描访客二维码方式授权访客使用网络；支持配置接待用户列表避免越权授权。 |
| 用户识别 | 支持对802.1X、华为controller、Kerberos、AD、POP3、Radius、数据库识别、PPPOE、华三iMC、城市热点、深澜计费等系统的单点登录。 |
| 审计日志 | 支持将多台设备日志集中存储于一台日志中心服务器，便于数据的集中查询与统计。日志中心支持选择Oracle数据库，访问日志中心数据必须采用https加密方式访问，避免传输过程被窃取。 |
| 对接接口 | 实现安全智能分析预警安全数据接口对接，为内部安全事件管理提供有效分析处理数据。 |

# （四）集成服务和其他要求

中标方须负责完成本项目涉及的整体规划、安装调试、服务实施等相关工作，须详细确认和理解采购人原有的系统情况、本次项目的建设目标和服务要求，并严格根据用户甲方项目进度安排完成实施工作，如有偏差由投标方负责。

**1.**投标时投标人需提供完整的系统集成实施方案、实施计划、项目管理规划等。

**2.**中标方负责本项目软硬件设备的供货、运输、保管、安装、调试、培训及售后服务等。

**3.**如集成实施过程中出现不符合招标文件要求的严重质量问题时，招标人保留索赔的权利。投标人根据项目实际需求，对系统集成实施方案进行统一设计、规划。

**4.**中标方需对整体项目方案的可行性负责，根据用户要求完成本项目的所有实施工作，解决实施过程中的全部技术问题。如在项目实施过程中出现无法实施或者缺少相关设备不能满足用户需求的情况应免费提供相关设备与配件。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，中标方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，由中标方负责。

**5.**中标方需配合用户完成漏洞通报、风险处置、事件处置等网络安全管理流程的梳理、设计工作。

**（五）项目组人员团队要求：**

项目组实施人员能力：投标人在浙江省内有常驻机构, 能提供快速的实施及售后服务，项目实施团队不少于10名工程师，其中具备工业和信息化部认证的“信息安全工程师”职业技术证书工程师3名以上。（须提供近三个月社保证明）

**商务要求表**

|  |  |  |
| --- | --- | --- |
| **▲供货时间（项目工期）及地点** | | 1．所有采购软件产品、硬件设备需在合同签订后30天内到货；  2．软件产品和硬件设备需在到货后5个月内完成安装、部署、调试、定制开发和上线。  3.正常试运行1个月，进行项目验收。  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）** | | 乙方在合同签订后5个工作日内向甲方支付合同总价5%的履约保证金，一年质保期满后30日内无服务质量问题索赔，无息退还乙方。  1.合同签订后7个工作日内，支付合同总金额的30%。  2．试运行满1个月后，支付合同总金额的50%。  3. 项目验收合格后7个工作日内，支付合同总金额的20%。 |
| **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** | 中标方应充分了解项目的实际需要和难度，确保设备正常运行，所有耗材由中标方提供。  1、 质量保证期  所有软硬件产品要求提供3年免费质保服务（到货验收合格之日起计）。  投标人须保证所提供产品符合国家有关规定，具有合法的版权或使用权，本项目采购的产品，如在本项目范围内使用过程中出现版权或使用权纠纷，应由中标人负责，采购人不承担责任。  中标方需在供货时提供硬件原厂商针对本项目的3年服务质保承诺函原件。  2、服务响应  软硬件故障响应时间1小时，故障修复时间2小时，4小时内无法修复，需提供应急替代方案。 |
| **响应情况** | 提供7X24小时电话、邮件、网站、传真等远程技术支持服务。 |
| **技术培训** | 中标方需合理安排与本项目实施相关的业务和技术培训，要求培训教师具备丰富的理论知识和实践经验。投标方应为用户指定的人员安排合适和足够的培训以使其在实施过程中有效参与并且在实施完成后顺利交接。 |
| **履约能力** | **公司技术力量情况** | 涉密信息系统集成资质乙级（含）以上3分；  ISO27001信息安全管理体系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，且至少能反映项目名称、与本次采购内容相似的合同内容、合同金额（原件备查）。（每提供一个得一份，最高3分） |

**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-119（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-119）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： 联系方式：

邮箱： 传真：

授权代表身份证号码：

法定代表人签名（或签名章）： 职务：

联系方式：

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-119（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：