**北京市政府采购项目**

**公开招标文件**

项目名称：网络视听新媒体综合监管平台升级改造项目

项目编号：11000024210200096601-XM001

项目代理编号：HCZB-2024-ZB1586

采 购 人：北京市广播电视监测中心

采购代理机构：华采招标集团有限公司

**目 录**

[第一章 投标邀请 2](#_Toc14497)

[第二章 投标人须知 6](#_Toc18952)

[第三章 资格审查 23](#_Toc24676)

[第四章 评标程序、评标方法和评标标准 27](#_Toc31501)

[第五章 采购需求 48](#_Toc6534)

[第六章 拟签订的合同文本 48](#_Toc7085)

[第七章 投标文件格式 128](#_Toc16825)

[一、资格证明文件格式 129](#_Toc14976)

[二、商务技术文件格式 143](#_Toc32278)

**第一章 投标邀请**

## 一、项目基本情况

1. 项目编号：11000024210200096601-XM001

项目代理编号：HCZB-2024-ZB1586

2.项目名称：网络视听新媒体综合监管平台升级改造项目

3.项目总预算金额：¥3085.556472万元

4.采购需求：

|  |  |  |  |
| --- | --- | --- | --- |
| 包号 | 包名称 | 包金额（万元） | 备注 |
| 第五包 | 行业网络安全监测业务建设（专网端） | 841.321172 | 软件部分预算金额：211.025万元；  设备部分预算金额：630.296172万元。 |
| 第六包 | 行业网络安全监测业务建设（互联网端） | 186.375 | 软件部分预算金额：49.875万元；  设备部分预算金额：136.5万元。 |

1. 合同履行期限：

第五包：合同签订后，60个自然日内，完成购置软硬件设备交货；合同签订后，180个自然日内，完成软件研发、部署、调试等工作。

第六包：合同签订后，60个自然日内，完成购置软硬件设备交货；合同签订后，180个自然日内，完成软件研发、部署、调试等工作。

6.本项目不接受联合体投标。

## 二、申请人的资格要求（须同时满足）

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求：

2.1 中小企业政策：

■本项目不专门面向中小企业预留采购份额。

□本项目专门面向 □中小 □小微企业 采购。即：提供的货物全部由符合政策 要求的中小/小微企业制造、服务全部由符合政策要求的中小/小微企业承接。

□本项目预留部分采购项目预算专门面向中小企业采购。对于预留份额，提供的货 物由符合政策要求的中小企业制造、服务由符合政策要求的中小企业承接。预留份额通过以下措施进行： / 。

2.2 其它落实政府采购政策的资格要求：无。

3.本项目的特定资格要求：

3.1本项目接受分支机构参与投标；

3.2本项目是否属于政府购买服务：

■否

□是，公益一类事业单位、使用事业编制且由财政拨款保障的群团组织，不得作为承接主体；

3.3其他特定资格要求：

（1）投标人必须为投标文件递交截止之日前未被列入“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；

（2）不同投标人的法人、单位负责人不是同一人也不存在直接控股、管理关系；

## 三、获取招标文件

1.时间：2024年10月25日至2024年11月01日，每天上午09:00至12:00，下午13:00至17:00（北京时间，法定节假日除外）。

2.地点：北京市政府采购电子交易平台

3.方式：供应商使用CA 数字证书或电子营业执照登录北京市政府采购电子交易平台（http://zbcg-bjzc.zhongcy.com/bjczj-portal-site/index.html#/home）获取电子版招标文件。

4.售价：0元。

## 四、提交投标文件截止时间、开标时间和地点

投标截止时间、开标时间：2024年11月15日09:30（北京时间）。

地点：北京市海淀区中关村东路18号财智国际大厦C栋20层 2010室第二会议室。

## 五、公告期限

自本公告发布之日起5个工作日。

## 六、其他补充事宜

1.本项目需要落实的政府采购政策：支持节能产品、环境标志产品、促进中小企业发展、支持监狱企业发展、促进残疾人就业等。

2. 本项目采用全流程线上线下结合采购方式，请供应商认真学习北京市政府采购电子交易平台发布的相关操作手册(供应商可在交易平台下载相关手册),办理 CA 数字证书或电子营业执照、进行北京市政府采购电子交易平台注册绑定，并认真核实CA数字证书或电子营业执照情况确认是否符合本项目电子化采购流程要求。

CA 数字证书服务热线 010-58511086

电子营业执照服务热线 400-699-7000

技术支持服务热线 010-86483801

2.1办理 CA 数字证书或电子营业执照

供应商登录北京市政府采购电子交易平台查阅“用户指南”—“操作指南”—“市场主体 CA 办理操作流程指引”/“电子营业执照使用指南”,按照程序要求办理。

2.2注册

供应商登录北京市政府采购电子交易平台“用户指南”—“操作指南”—“市场主体注册入库操作流程指引”进行自助注册绑定。

2.3驱动、客户端下载

供应商登录北京市政府采购电子交易平台“用户指南”—“工具下载”—“招标采购系统文件驱动安装包”下载相关驱动。

供应商登录北京市政府采购电子交易平台“用户指南”—“工具下载”—“投标文件编制工具”下载相关客户端。

2.4获取电子招标文件

供应商使用CA 数字证书或电子营业执照登录北京市政府采购电子交易平台获取电子招标文件。

供应商如计划参与多个采购包的投标，应在登录北京市政府采购电子交易平台后，在【我的项目】栏目依次选择对应采购包，进入项目工作台招标/采购文件环节分别按采购包下载招标文件电子版。

3.本公告同时在中国政府采购网（http://www.ccgp.gov.cn）、北京市政府采购网（http://www.ccgp-beijing.gov.cn/）上发布。

## 七、对本次招标提出询问，请按以下方式联系。

**1.采购人信息**

名 称：北京市广播电视监测中心

地 址：北京市通州区达济街5号院

联系方式：殷老师 010-55565330

**2.采购代理机构信息**

名 称：华采招标集团有限公司

地　址：北京市丰台区广安路9号国投财富广场6号楼1601室

联系方式：贾东敏、姚冲、刘金秀18612287813/18612287807

**3.项目联系方式**

项目联系人：贾东敏、姚冲、刘金秀

项目联系方式：18612287813/18612287807

**第二章 投标人须知**

## 投标人须知资料表

本表是对投标人须知的具体补充和修改，如有矛盾，均以本资料表为准。

| **条款号** | **条目** | **内容** |
| --- | --- | --- |
| 2.2 | 项目属性 | 第五包、第六包：货物采购 |
| 2.3 | 科研仪器设备 | 是否属于科研仪器设备采购项目：否 |
| 2.4 | 核心产品 | ■本项目五包为非单一产品采购项目，核心产品为： 日志探针；  本项目六包为非单一产品采购项目，核心产品为： 日志探针。 |
| 3.1 | 现场考察 | 不组织 |
| 开标前答疑会 | 不召开 |
| 4.1 | 样品 | 投标样品递交：不需要 |
| 5.2.5 | 标的所属行业 | 本项目采购标的对应的中小企业划分标准所属行业：  第五包：工业  第六包：工业 |
| 11.2 | 投标报价 | 投标报价的特殊规定：无 |
| 12.1 | 投标保证金 | 投标保证金金额：第五包：8万元；第六包：1万元。  递交时间：同首次递交投标文件截止时间（逾期递交按无效投标处理）  递交地点：华采招标集团有限公司（北京市丰台区广安路9号国投财富广场6号楼1601室）。  投标保证金形式：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。  投标保证金收受人信息：  **户 名：华采招标集团有限公司**  **开 户 行：建行北京西客站支行（仅限投标保证金）**  **账 号：1105 0165 5100 0000 0292（请备注：ZB1586保证金）**  退还投标保证金形式：电汇形式 |
| 12.7.2 | 投标保证金可以不予退还的其他情形：无 |
| 13.1 | 投标有效期 | 自提交投标文件的截止之日起算90日历天。 |
| 14.1 | 投标文件签署、盖章 | 投标文件资格册：正本：1份，副本：5份，电子版：1份。  投标文件商务技术册：正本：1份，副本：5份，电子版：1份。  （电子文件须提供**可编辑word文档和PDF**加盖公章扫描版文件，存储载体为U盘）  电子文件规定格式为：  （1）文本文件采用DOC、RTF、TXT、PDF格式；  （2）图像文件采用JPEG、TIFF格式；  （3）影像文件采用MPEG、AVI格式；  （4）声音文件采用WAV、MP3格式。  **注：投标文件一律采用A4幅面（图纸、彩页等除外），左侧装订。装订应牢固紧密，不易松动散落，不得采用活页式装订，采购人或采购代理机构对因装订不牢造成的文件散失不负责任。副本可以是正本的复印件。** |
| 22.1 | 确定中标人 | 中标候选人并列的，按照以下方式确定中标人：  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并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。 |
| 25.5 | 分包 | 本项目的非主体、非关键性工作是否允许分包：不允许 |
| 26.1.1 | 询问 | 询问送达形式：书面形式 |
| 26.3 | 联系方式 | 接收询问和质疑的联系方式  联系部门：华采招标集团有限公司；  联系电话：18612287813/18612287807；  通讯地址：北京市丰台区广安路9号国投财富广场6号楼1601室。  邮 箱：hczb104@163.com  联 系 人： 贾东敏 |
| 27 | 代理费 | 中标人须向采购代理机构按如下标准和规定交纳成交服务费。  （1）以中标金额作为收费的计算基数。  （2）采购代理机构按《招标代理服务收费管理暂行办法》（计价格[2002]1980号）及《国家发展改革委办公厅关于招标代理服务收费有关问题的通知》（发改办价格[2003]857号）下浮10%执行，按成交金额差额定率累进法计算，由成交供应商支付。造价咨询服务费，按照北京市建设工程造价管理协会（京价协【2015】011号）《关于调整“北京市建设工程造价咨询服务参考费用及费用指数”》后的解释和自律管理的文件规定，记取造价服务费，由成交供应商支付。  （3）成交服务费币种与成交签订合同的币种相同或采购代理机构同意的币种。  （4）成交服务费的交纳方式：  在递交响应文件时，供应商向采购代理机构送交成交服务费承诺书。成交供应商在领取成交通知书时一次性向采购代理机构交纳所有成交服务费。  **服务费汇款账户：（交纳成交服务费时请备注ZB1586）**  **账户名称：华采招标集团有限公司**  **开户银行：建设银行北京保福寺支行**  **账户号码：11050163990000000889**  **行号：1051 0005 0245** |

**投标人须知**

## 一 说 明

1. 采购人、采购代理机构、投标人、联合体
   1. 采购人、采购代理机构：指依法进行政府采购的国家机关、事业单位、团体组织，及其委托的采购代理机构。本项目采购人、采购代理机构见第一章《投标邀请》。
   2. 投标人（也称“供应商”、“申请人”）：指向采购人提供货物、工程或者服务的法人、其他组织或者自然人。
   3. 联合体：指两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购。
2. 资金来源、项目属性、科研仪器设备采购、核心产品
   1. 资金来源为财政性资金和/或本项目采购中无法与财政性资金分割的非财政性资金。
   2. 项目属性见《投标人须知资料表》。
   3. 是否属于科研仪器设备采购见《投标人须知资料表》。
   4. 核心产品见《投标人须知资料表》。
3. 现场考察、开标前答疑会
   1. 若《投标人须知资料表》中规定了组织现场考察、召开开标前答疑会，则投标人应按要求在规定的时间和地点参加。
   2. 由于未参加现场考察或开标前答疑会而导致对项目实际情况不了解，影响投标文件编制、投标报价准确性、综合因素响应不全面等问题的，由投标人自行承担不利评审后果。
4. 样品
   1. 本项目是否要求投标人提供样品，以及样品制作的标准和要求、是否需要随样品提交相关检测报告、样品的递交与退还等要求见《投标人须知资料表》。
   2. 样品的评审方法以及评审标准等内容见第四章《评标方法和评标标准》。
5. 政府采购政策（包括但不限于下列具体政策要求）
   1. 进口产品
      1. 指通过中国海关报关验放进入中国境内且产自关境外的产品，包括已经进入中国境内的进口产品。关于进口产品的相关规定依据《政府采购进口产品管理办法》（财库〔2007〕119号文）、《关于政府采购进口产品管理有关问题的通知》（财办库〔2008〕248号文）。
      2. 本项目是否接受进口产品见第五章《采购需求》。
   2. 中小企业、监狱企业及残疾人福利性单位
      1. 中小企业定义：
         1. 中小企业是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。关于中小企业的相关规定依据《中华人民共和国中小企业促进法》、《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）、《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）、《国务院关于进一步促进中小企业发展的若干意见》（国发〔2009〕36 号）。
         2. 供应商提供的货物、工程或者服务符合下列情形的，享受中小企业扶持政策：

（1）在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

（2）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

（3）在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。

* + - 1. 在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受中小企业扶持政策。
      2. 以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。
    1. 监狱企业定义：是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地（设区的市）监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。
    2. 残疾人福利单位定义：享受政府采购支持政策的残疾人福利性单位应当同时满足以下条件：
       1. 安置的残疾人占本单位在职职工人数的比例不低于25%（含25%），并且安置的残疾人人数不少于10 人（含10 人）；
       2. 依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；
       3. 为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；
       4. 通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；
       5. 提供本单位制造的货物、承担的工程或者服务（以下简称产品），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）；
       6. 前款所称残疾人是指法定劳动年龄内，持有《中华人民共和国残疾人证》或者《中华人民共和国残疾军人证（1 至8 级）》的自然人，包括具有劳动条件和劳动意愿的精神残疾人。在职职工人数是指与残疾人福利性单位建立劳动关系并依法签订劳动合同或服务协议的雇员人数。
    3. 本项目是否专门面向中小企业预留采购份额见第一章《投标邀请》。
    4. 采购标的对应的中小企业划分标准所属行业见《投标人须知资料表》。
    5. 小微企业价格评审优惠的政策调整：见第四章《评标方法和评标标准》。
  1. 政府采购节能产品、环境标志产品
     1. 政府采购节能产品、环境标志产品实施品目清单管理。财政部、发展改革委、生态环境部等部门根据产品节能环保性能、技术水平和市场成熟程度等因素，确定实施政府优先采购和强制采购的产品类别及所依据的相关标准规范，以品目清单的形式发布并适时调整。依据品目清单和认证证书实施政府优先采购和强制采购。
     2. 采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。关于政府采购节能产品、环境标志产品的相关规定依据《关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）。
     3. 如本项目采购产品属于实施政府强制采购品目清单范围的节能产品，则投标人所报产品必须获得国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，否则**投标无效**；
     4. 非政府强制采购的节能产品或环境标志产品，依据品目清单和认证证书实施政府优先采购。优先采购的具体规定见第四章《评标方法和评标标准》（如涉及）。
  2. 支持乡村产业振兴管理
     1. 为落实《关于运用政府采购政策支持乡村产业振兴的通知》（财库〔2021〕19号）有关要求，做好支持脱贫攻坚工作，本项目采购活动中对于支持乡村振兴管理的相关要求见第五章《采购需求》（如涉及）。
  3. 正版软件
     1. 。国家有特殊信息安全要求的项目，采购产品涉及无线局域网产品和含有无线局域网功能的计算机、通信设备、打印机、复印机、投影仪等产品的，投标产品须为符合国家无线局域网安全标准(GB 15629.11/1102-2003)并符合《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求。
     2. 各级政府部门在购置计算机办公设备时，必须采购预装正版操作系统软件的计算机产品，相关规定依据《国家版权局、信息产业部、财政部、国务院机关事务管理局关于政府部门购置计算机办公设备必须采购已预装正版操作系统软件产品的通知》（国权联〔2006〕1 号）、《国务院办公厅关于进一步做好政府机关使用正版软件工作的通知》（国办发〔2010〕47 号）、《财政部关于进一步做好政府机关使用正版软件工作的通知》（财预〔2010〕536 号）。
  4. 网络安全专用产品
     1. 所投产品属于列入《网络关键设备和网络安全专用产品目录》的网络 安全专用产品，应当在国家互联网信息办公室会同工业和信息化部、 公安部、国家认证认可监督管理委员会统一公布和更新的符合要求的 网络关键设备和网络安全专用产品清单中。
  5. 推广使用低挥发性有机化合物（VOCs）
     1. 为全面推进本市挥发性有机物（VOCs）治理，贯彻落实挥发性有机物污染治理专项行动有关要求，相关规定依据《北京市财政局北京市生态环境局关于政府采购推广使用低挥发性有机化合物（VOCs）有关事项的通知》（京财采购〔2020〕2381 号）。本项目中涉及涂料、胶黏剂、油墨、清洗剂等挥发性有机物产品的，属于强制性标准的，供应商应执行符合本市和国家的VOCs 含量限制标准（具体标准见第五章《采购需求》），否则**投标无效**；属于推荐性标准的，优先采购，具体见第四章《评标方法和评标标准》。

1. 投标费用
   1. 投标人应自行承担所有与准备和参加投标有关的费用，无论投标的结果如何，采购人或采购代理机构在任何情况下均无承担这些费用的义务和责任。

## 二 招标文件

1. 招标文件构成
   1. 招标文件包括以下部分：
2. 投标邀请
3. 投标人须知
4. 资格审查
5. 评标程序、评标方法和评标标准
6. 采购需求
7. 拟签订的合同文本
8. 投标文件格式
   1. 投标人应认真阅读招标文件的全部内容。投标人应按照招标文件要求提交投标文件并保证所提供的全部资料的真实性，并对招标文件作出实质性响应，否则**投标无效**。
9. 对招标文件的澄清或修改
   1. 采购人或采购代理机构对已发出的招标文件进行必要澄清或者修改的，将在原公告发布媒体上发布更正公告，并以书面形式通知所有获取招标文件的潜在投标人。
   2. 上述书面通知，按照获取招标文件的潜在投标人提供的联系方式发出，因提供的信息有误导致通知延迟或无法通知的，采购人或采购代理机构不承担责任。
   3. 澄清或者修改的内容为招标文件的组成部分，并对所有获取招标文件的潜在投标人具有约束力。澄清或者修改的内容可能影响投标文件编制的，将在投标截止时间至少15日前，以书面形式通知所有获取招标文件的潜在投标人；不足15日的，将顺延提交投标文件的截止时间和开标时间。

## 三 投标文件的编制

1. 投标范围、投标文件中计量单位的使用及投标语言
   1. 本项目如划分采购包，投标人可以对本项目的其中一个采购包进行投标，也可同时对多个采购包进行投标。投标人应当对所投采购包对应第五章《采购需求》所列的全部内容进行投标，不得将一个采购包中的内容拆开投标，否则其对该采购包的投标将被认定为**无效投标**。
   2. 除招标文件有特殊要求外，本项目投标所使用的计量单位，应采用中华人民共和国法定计量单位。
   3. 除专用术语外，投标文件及来往函电均应使用中文书写。必要时专用术语应附有中文解释。投标人提交的支持资料和已印制的文献可以用外文，但相应内容应附有中文翻译本，在解释投标文件时以中文翻译本为准。未附中文翻译本或翻译本中文内容明显与外文内容不一致的，其不利后果由投标人自行承担。
2. 投标文件构成
   1. 投标人应当按照招标文件的要求编制投标文件。投标文件应由《资格证明文件》、《商务技术文件》两部分构成。投标文件的部分格式要求，见第七章《投标文件格式》。
   2. 对于招标文件中标记了“实质性格式”文件的，投标人不得改变格式中给定的文字所表达的含义，不得删减格式中的实质性内容，不得自行添加与格式中给定的文字内容相矛盾的内容，不得对应当填写的空格不填写或不实质性响应，否则**投标无效**。未标记“实质性格式”的文件和招标文件未提供格式的内容，可由投标人自行编写。
   3. 第四章《评标程序、评标方法和评标标准》中涉及的证明文件。
   4. 对照第五章《采购需求》，说明所提供货物和服务已对第五章《采购需求》做出了响应，或申明与第五章《采购需求》的偏差和例外。如第五章《采购需求》中要求提供证明文件的，投标人应当按具体要求提供证明文件。
   5. 投标人认为应附的其他材料。
3. 投标报价
   1. 所有投标均以人民币报价。
   2. 投标人的报价应包括为完成本项目所发生的一切费用和税费，招标人将不再支付报价以外的任何费用。投标人的报价应包括但不限于下列内容，《投标人须知资料表》中有特殊规定的，从其规定。
      1. 投标货物及标准附件、备品备件、专用工具等的出厂价（包括已在中国国内的进口货物完税后的仓库交货价、展示交货价或货架交货价）和运至最终目的地的运输费和保险费，安装调试、检验、技术服务、培训、质量保证、售后服务、税费等按照招标文件要求完成本项目的全部相关服务费用；
      2. 按照招标文件要求完成本项目的全部相关服务费用。
   3. 采购人不得向供应商索要或者接受其给予的赠品、回扣或者与采购无关的其他商品、服务。
   4. 投标人不能提供任何有选择性或可调整的报价，否则其**投标无效**。
4. 投标保证金
   1. 投标人应按《投标人须知资料表》中规定的金额及要求交纳投标保证金，并作为其投标的一部分。
   2. 交纳投标保证金可采用的形式：政府采购法律法规接受的支票、汇票、本票、网上银行支付或者金融机构、担保机构出具的保函等非现金形式。
   3. 投标保证金到账（保函提交）截止时间同投标截止时间。以支票、汇票、本票、网上银行支付等形式提交投标保证金的，应在投标截止时间前到账；以金融机构、担保机构出具的保函等形式提交投标保证金的，应在投标截止时间前将原件提交至采购代理机构。由于到账时间晚于投标截止时间的，或者票据错误、印鉴不清等原因导致不能到账的，其**投标无效**。
   4. 投标保证金（保函）有效期同投标有效期。
   5. 联合体投标的，可以由联合体中的一方或者共同提交投标保证金，以一方名义提交投标保证金的，对联合体各方均具有约束力。
   6. 采购人、采购代理机构将及时退还投标人的投标保证金，采用银行保函、担保机构担保函等形式递交的投标保证金，经供应商同意后采购人、采购代理机构可以不再退还，但因投标人自身原因导致无法及时退还的除外：
      1. 投标人在投标截止时间前撤回已提交的投标文件的，自收到投标人书面撤回通知之日起5个工作日内退还已收取的投标保证金；
      2. 中标人的投标保证金，自采购合同签订之日起5个工作日内退还中标人；
      3. 未中标投标人的投标保证金，自中标通知书发出之日起5个工作日内退还未中标人；
      4. 终止招标项目已经收取投标保证金的，自终止采购活动后5个工作日内退还已收取的投标保证金及其在银行产生的孳息。
   7. 有下列情形之一的，采购人或采购代理机构可以不予退还投标保证金：
      1. 投标有效期内投标人撤销投标文件的；
      2. 《投标人须知资料表》中规定的其他情形。
5. 投标有效期
   1. 投标文件应在本招标文件《投标人须知资料表》中规定的投标有效期内保持有效，投标有效期少于招标文件规定期限的，其**投标无效**。
6. 投标文件的签署、盖章
   1. 投标人应按招标文件第二章投标人须知资料表的规定准备投标文件的正本、副本、电子版，每份投标文件须清楚地标明“正本”、“副本”、“电子版”。副本可以为正本的复印件，若正本和副本、电子文件不符，以纸质正本为准。投标文件可双面打印。
   2. 投标文件的正本需打印或用不褪色墨水书写。
   3. 任何对投标文件行间插字、涂改和增删，必须由法定代表人或其授权代表签字或加盖本单位公章后有效。
   4. 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。
   5. 招标文件中所要求加盖的投标人公章是指与投标人名称全称相一致的“行政公章”，不得加盖其他“合同专用章、投标专用章、财务专用章”等非行政公章，否则将被视为无效投标。

## 四 投标文件的提交

1. 投标文件的提交
   1. 投标文件一律采用A4幅面（图纸、彩页等除外）左侧装订。装订应牢固紧密，不易散落，不得采用活页式装订，采购人或采购代理机构对因装订不牢造成的文件散失不负责任。响应文件可双面打印。
   2. 投标人应将“开标一览表”、“投标文件资格册正本”、“投标文件资格册副本”、“投标文件商务技术册正本”、“投标文件商务技术册副本”、“投标保证金复印件（如有）”、“投标文件电子版”、“样品（如有）”分开单独密封，并在密封袋/箱上分别标明“开标一览表”、“投标文件资格册正本”、“投标文件资格册副本”、“投标保证金复印件（如有）”、“投标文件电子版”、“投标文件商务技术册正本”、“投标文件商务技术册副本”、“样品（如有）”字样，在投标时统一提交。
   3. 所有密封袋/箱上均应：

1）清楚标明投标文件递交地点暨开标地点。

2）注明招标的项目名称、项目代理编号和投标人名称和地址，以及“在（开标时间）之前不得启封”的字样。如果投标人未按上述要求加写标记的，采购代理机构对投标文件的误投概不负责。

15.4 投标人根据招标文件要求编制并提交投标文件

1. 投标截止时间
   1. 投标人应在招标文件要求提交投标文件截止时间前，将投标文件按招标公告或投标邀请书中规定的投标地点递交。
2. 投标文件的修改与撤回
   1. 投标截止时间前，投标人可以对所提交的投标文件进行补充、修改或者撤回。并修改或者撤回通知采购人或采购代理机构。
   2. 投标人对投标文件的补充、修改的内容应当按照招标文件要求签署、盖章，作为投标文件的组成部分。

## 五 开标、资格审查及评标

1. 开标
   1. 采购人或采购代理机构将按招标文件的规定，在投标截止时间的同一时间和招标文件预先确定的地点组织开标。
   2. 开标过程将宣布投标人名称、投标价格和招标文件规定的需要宣布的其他内容并进行记录，并由参加开标的各投标人代表确认。
   3. 投标人代表对开标过程和开标记录有疑义，以及认为采购人、采购代理机构相关工作人员有需要回避的情形的，应当场提出询问或者回避申请。采购人、采购代理机构对投标人代表提出的询问或者回避申请将及时处理。
   4. 投标人不足3家的，不予开标。
2. 资格审查
   1. 见第三章《资格审查》。
3. 评标委员会
   1. 评标委员会根据政府采购有关规定和本次招标采购项目的特点进行组建，并负责具体评标事务，独立履行职责。
   2. 评审专家须符合《财政部关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125号）的规定。依法自行选定评审专家的，采购人和采购代理机构将查询有关信用记录，对具有行贿、受贿、欺诈等不良信用记录的人员，拒绝其参与政府采购活动。
4. 评标程序、评标方法和评标标准
   1. 见第四章《评标程序、评标方法和评标标准》。

## 六 确定中标

1. 确定中标人
   1. 采购人将在评标报告确定的中标候选人名单中按顺序确定中标人，中标候选人并列的，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中标人；招标文件未规定的，采取随机抽取的方式确定。采购人是否委托评标委员会直接确定中标人，见《投标人须知资料表》。中标候选人并列的，按照《投标人须知资料表》要求确定成交供应商。
2. 中标公告与中标通知书
   1. 采购人或采购代理机构自中标人确定之日起2个工作日内，在北京市政府采购网公告中标结果，同时向中标人发出中标通知书，中标公告期限为1个工作日。
   2. 中标通知书对采购人和中标供应商均具有法律效力。中标通知书发出后，采购人改变中标结果的，或者中标供应商放弃中标项目的，应当依法承担法律责任。
3. 废标
   1. 在招标采购中，出现下列情形之一的，应予废标：
      1. 符合专业条件的供应商或者对招标文件作实质响应的供应商不足三家的；
      2. 出现影响采购公正的违法、违规行为的；
      3. 投标人的报价均超过了采购预算，采购人不能支付的；
      4. 因重大变故，采购任务取消的。
   2. 废标后，采购人将废标理由通知所有投标人。
4. 签订合同
   1. 中标人、采购人应当自中标通知书发出之日起30日内，按照招标文件和中标人投标文件的规定签订书面合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。
   2. 中标人拒绝与采购人签订合同的，采购人可以按照评标报告推荐的中标候选人名单排序，确定下一候选人为中标人，也可以重新开展政府采购活动。
   3. 联合体中标的，联合体各方应当共同与采购人签订合同，就中标项目向采购人承担连带责任。
   4. 政府采购合同不能转包。
   5. 采购人允许采用分包方式履行合同的，中标人可以依法在中标后将中标项目的非主体、非关键性工作采取分包方式履行合同。本项目的非主体、非关键性工作是否允许分包，见《投标人须知资料表》。政府采购合同分包履行的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包**，**否则**投标无效**。中标人就采购项目和分包项目向采购人负责，分包供应商就分包项目承担责任。
5. 询问与质疑
   1. 询问
      1. 投标人对政府采购活动事项有疑问的，可依法提出询问，并按《投标人须知资料表》载明的形式送达采购人或采购代理机构。
      2. 采购人或采购代理机构对供应商依法提出的询问，在3个工作日内作出答复，但答复的内容不得涉及商业秘密。
   2. 质疑
      1. 投标人认为采购文件、采购过程、中标结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，由投标人派授权代表以书面形式向采购人、采购代理机构提出质疑。采购人、采购代理机构在收到质疑函后7个工作日内作出答复。
      2. 质疑函须使用财政部制定的范本文件。
      3. 投标人为自然人的，应当由本人签字；投标人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。
      4. 投标人应在法定质疑期内一次性提出针对同一采购程序环节的质疑，法定质疑期内针对同一采购程序环节再次提出的质疑，采购人、采购代理机构有权不予答复。
   3. 接收询问和质疑的联系部门、联系电话和通讯地址见《投标人须知资料表》。
6. 代理费
   1. 收费对象、收费标准及缴纳时间见《投标人须知资料表》。由中标人支付的，中标人须一次性向采购代理机构缴纳代理费，投标报价应包含代理费用。

**第三章 资格审查**

**一、资格审查程序**

1. 开标结束后，采购人或采购代理机构将根据《资格审查要求》中的规定，对投标人进行资格审查，并形成资格审查结果。
2. 《资格审查要求》中对格式有要求的，除招标文件另有规定外，均为“实质性格式”文件。
3. 投标人《资格证明文件》有任何一项不符合《资格审查要求》的，资格审查不合格，其**投标无效**。
4. 资格审查合格的投标人不足3家的，不进行评标。

**二、资格审查要求**

| **序号** | **审查因素** | **审查内容** | **格式要求** |
| --- | --- | --- | --- |
| 1 | 满足《中华人民共和国政府采购法》第二十二条规定及法律法规的其他规定 | 具体规定见第一章《投标邀请》 |  |
| 1-1 | 营业执照等证明文件 | 投标人为企业（包括合伙企业）的，应提供  有效的营业执照଀；  投标人为事业单位的，应提供有效的“事业单  位法人证书“；  投标人是非企业机构的，应提供有效的“营业  许可证“、“登记证书”等证明文件；  投标人是个体工商户的，应提供有效的“个体  工商户营业执照”；  投标人是自然人的，应提供有效的自然人身  份证明。  分支机构参加投标的，应提供该分支机构或  其所属法人/其他组织的相应证明文件；同时  还应提供其所属法人/其他组织出具的授权  其参与本项目的授权书（格式自拟，须加盖  其所属法人/其他组织的公章）；对于银行、  保险、石油石化、电力、电信等行业的分支  机构，可以提供上述授权，也可以提供其所  属法人/其他组织的有关文件或制度等能够  证明授权其独立开展业务的证明材料。 | 提供证明文件的电子件或电子证照 |
| 1-2 | 投标人资格声明书 | 提供了符合招标文件要求的《投标人资格声明书》。 | 格式见《投标文件格式》 |
| 1-3 | 投标人信用记录 | 查询渠道：信用中国网站和中国政府采购网（www.creditchina.gov.cn、www.ccgp.gov.cn）；  截止时点：投标截止时间以后、资格审查阶段采购人或采购代理机构的实际查询时间；  信用信息查询记录和证据留存具体方式：查询结果网页打印页作为查询记录和证据，与其他采购文件一并保存；  信用信息的使用原则：经认定的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投标人，其**投标无效**。联合体形式投标的，联合体成员存在不良信用记录，视同联合体存在不良信用记录。 | 无须投标人提供，由采购人或采购代理机构查询。 |
| 2 | 落实政府采购政策需满足的资格要求 | 具体要求见第一章《投标邀请》 |  |
| 2-1 | 中小企业声明函 | 当本项目（包）涉及预留份额专门面向中小企业采购，应在《资格证明文件》中提供。  1、投标人单独投标的，应提供中小企业声明函；如为监狱企业或残疾人福利性单位，不必提供中小企业声明函，但须按注1或注2要求提供证明材料。  2、如招标文件要求以联合体形式参加或者要求合同分包的，且投标人为联合体或拟进行合同分包的，则联合体中的中小企业、签订分包意向协议的中小企业具体情况须在《中小企业声明函》中如实填报。上述中小企业如为监狱企业或残疾人福利性单位应在声明函中如实列明单位性质，并按注1或注2要求提供证明材料。  注1：监狱企业须提供由省级以上监狱管理局（北京市含教育矫治局）、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。  注2：残疾人福利性单位须按招标文件要求提供《残疾人福利性单位声明函》。 | 格式见《投标文件格式》 |
| 2-2 | 拟分包情况说明及分包意向协议（类型一） | 如本项目（包）要求通过分包措施预留部分采购份额面向中小企业采购、且投标人因落实政府采购政策拟进行分包的，必须提供；否则无须提供。  对于预留份额专门面向中小企业采购的项目（包），组成联合体或者接受分包合同的中小企业与联合体内其他企业、分包企业之间不得存在直接控股、管理关系。 | 格式见《投标文件格式》 |
| 2-3 | 其它落实政府采购政策的资格要求 | 见第一章《投标邀请》 | 提供证明文件的扫描件或复印件 |
| 3 | 本项目的特定资格要求 | 见第一章《投标邀请》 | 提供证明文件的扫描件或复印件 |
| 3-1 | 是否接受联合体投标 | 1、如本项目接受联合体投标，且投标人为联合体时必须提供《联合协议》，明确各方拟承担的工作和责任，并指定联合体牵头人，授权其代表所有联合体成员负责本项目投标和合同实施阶段的牵头、协调工作。该联合协议应当作为投标文件的组成部分，与投标文件其他内容同时递交。  2、联合体各成员单位均须提供本表中序号1-1、1-2的证明文件。  3、本表序号3-2项规定的其他特定资格要求中的每一小项要求，联合体各方中至少应当有一方符合本表中其他资格要求并提供证明文件。  4、联合体中有同类资质的供应商按照联合体分工承担相同工作的，应当按照资质等级较低的供应商确定资质等级。  5、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。  6、若联合体中任一成员单位中途退出，则该联合体的**投标无效**。  7、本项目不接受联合体投标时，投标人不得为联合体。 | 提供《联合协议》原件的扫描件或复印件  格式见《投标文件格式》 |
| 3-2 | 其他特定资格要求 | 见第一章《投标邀请》 | 提供证明文件的扫描件或复印件 |
| 4 | 投标保证金 | 按照招标文件的规定提交投标保证金。 |  |

**第四章** **评标程序、评标方法和评标标准**

**一、评标方法**

1. 投标文件的符合性审查
   1. 评标委员会对资格审查合格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。
   2. 评标委员会根据《符合性审查要求》中规定的审查因素和审查内容，对投标人的投标文件是否实质上响应招标文件进行符合性审查，并形成符合性审查评审结果。投标人《商务技术文件》有任何一项不符合《符合性审查要求》要求的，**投标无效**。

**符合性审查要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **审查因素** | **审查内容** |
| 1 | 授权委托书 | 按招标文件要求提供授权委托书 |
| 2 | 投标完整性 | 未将一个采购包中的内容拆分投标； |
| 3 | 投标报价 | 投标报价未超过招标文件中规定的项目/采购包预算金额或者 项目/采购包最高限价； |
| 4 | 报价唯一性 | 投标文件未出现可选择性或可调整的报价(招标文件另有规定 的除外); |
| 5 | 投标有效期 | 投标文件中承诺的投标有效期满足招标文件中载明的投标有效 期 的 ； |
| 6 | 实质性格式 | 标记为“实质性格式”的文件均按招标文件要求提供且签署、盖 章 的 ； |
| 7 | ★号条款响应 | 投标文件满足招标文件第五章《采购需求》中★号条款要求的； |
| 8 | 拟分包情况说 明(如有) | 如本项目(包)非因“落实政府采购政策”亦允许分包，且供应商拟进行分包时，必须提供；否则无须提供； |
| 9 | 分包其他要求 (如有) | 分包履行的内容、金额或者比例未超出《投标人须知资料表》  中的规定；  分包承担主体具备《投标人须知资料表》载明的资质条件且提 供了资质证书电子件(如有); |
| 10 | 报价的修正(如 有 ) | 不涉及报价修正，或投标文件报价出现前后不一致时，投标人 对修正后的报价予以确认；(如有) |
| 11 | 报价合理性 | 报价合理，或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的，能够应 评标委员会要求在规定时间内证明其报价合理性的； |
| 12 | 进口产品  (如有) | 招标文件不接受进口产品投标的内容时，投标人所投产品不含 进口产品； | |
| 13 | 国家有关部门 对投标人的投  标产品有强制  性规定或要求  的 | 国家有关部门对投标人的投标产品有强制性规定或要求的(如 相应技术、安全、节能和环保等),投标人的投标产品应符合 相应规定或要求，并提供证明文件电子件：  1)采购的产品若属于《节能产品政府采购品目清单》范围中 政府强制采购产品，则投标人所报产品必须获得国家确定的认 证机构出具的、处于有效期之内的节能产品认证证书；  2)所投产品属于列入《网络关键设备和网络安全专用产品目  录》的网络安全专用产品时，应当按照《信息安全技术网络安 全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求；(如该产品已经获得公安部颁发的计算机信息系统安全专用产品销售许 可证，且在有效期内，亦视为符合要求)  3)国家有特殊信息安全要求的项目，采购产品涉及无线局域  网产品和含有无线局域网功能的计算机、通信设备、打印机、 复印机、投影仪等产品的，投标产品须为符合国家无线局域网 安全标准(GB15629.11/1102-2003)并符合《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求。；  4)项目中涉及涂料、胶黏剂、油墨、清洗剂等挥发性有机物  产品，且属于强制性标准的，供应商应执行符合本市和国家的 VOCs含量限制标准。 | |
| 14 | 公平竞争 | 投标人遵循公平竞争的原则，不存在恶意串通，妨碍其他投标  人的竞争行为，不存在损害采购人或者其他投标人的合法权益情形的 ； | |
| 15 | 串通投标 | 不存在《政府采购货物和服务招标投标管理办法》视为投标人  串通投标的情形：  (一)不同投标人的投标文件由同一单位或者 个人编制；  (二)不同投标人委托同一单位或者个人办理投标事宜；  (三)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；  (四)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；  (五)不同投标人的投标文件相互混装；  (六) 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。 | |
| 16 | 附加条件 | 投标文件未含有采购人不能接受的附加条件的； | |
| 17 | 其他无效情形 | 投标人、投标文件不存在不符合法律、法规和招标文件规定的 其他无效情形。 | |

1. 投标文件有关事项的澄清或者说明
   1. 评标过程中，评标委员会将以书面形式要求投标人对其投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，作出必要的澄清、说明或者补正。投标人的澄清、说明或者补正应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字。投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。澄清文件将作为投标文件内容的一部分。
   2. 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的，有权要求该投标人在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；若投标人不能证明其报价合理性，评标委员会将其作为**无效投标处理**。
   3. 投标报价须包含招标文件全部内容，如分项报价表有缺漏视为已含在其他各项报价中，将不对投标总价进行调整。评标委员会有权要求投标人在评标现场合理的时间内对此进行书面确认，投标人不确认的，视为将一个采购包中的内容拆开投标，其**投标无效**。
   4. 投标文件报价出现前后不一致的，按照下列规定修正：
      1. 招标文件对于报价修正是否另有规定：

□有，具体规定为：\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**■**无，按下述2.4.2-2.4.7项规定修正。

* + 1. 单独递交的开标一览表（报价表）与投标文件中开标一览表（报价表）内容不一致的，以单独递交的开标一览表（报价表）为准；
    2. 投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；
    3. 大写金额和小写金额不一致的，以大写金额为准；
    4. 单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价；
    5. 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。
    6. 同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价经投标人书面确认后产生约束力，投标人不确认的，其**投标无效**。
  1. 落实政府采购政策的价格调整：只有符合第二章《投标人须知》5.2条规定情形的，可以享受中小企业扶持政策，用扣除后的价格参加评审；否则，评标时价格不予扣除。
     1. 对于未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对小微企业报价给予10%的扣除，用扣除后的价格参加评审。
     2. 对于未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，且接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额 30%以上的联合体或者大中型企业的报价给予4%的扣除，用扣除后的价格参加评审。
     3. 组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。
     4. 价格扣除比例对小型企业和微型企业同等对待，不作区分。
     5. 中小企业参加政府采购活动，应当按照招标文件给定的格式出具《中小企业声明函》，否则不得享受相关中小企业扶持政策。
     6. 监狱企业提供了由省级以上监狱管理局（北京市含教育矫治局）、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的，视同小微企业。
     7. 残疾人福利性单位按招标文件要求提供了《残疾人福利性单位声明函》（见附件）的，视同小微企业。
     8. 若投标人同时属于小型或微型企业、监狱企业、残疾人福利性单位中的两种及以上，将不重复享受小微企业价格扣减的优惠政策。

1. 投标文件的比较和评价
   1. 评标委员会将按照招标文件中规定的评标方法和标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价；未通过符合性审查的投标文件不得进入比较与评价。
   2. 评标方法和评标标准
      1. 本项目采用的评标方法为：

**■**综合评分法，指投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法，见《评标标准》，招标文件中没有规定的评标标准不得作为评审的依据。

□最低评标价法，指投标文件满足招标文件全部实质性要求，且投标报价最低的投标人为中标候选人的评标方法。

* + 1. 采用最低评标价法时，提供相同品牌产品（单一产品或核心产品品牌相同）的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会按照下述方法确定一个参加评标的投标人，其他**投标无效**。

□随机抽取

□其他方式，具体要求：\_\_\_\_\_

* + 1. 非政府强制采购的节能产品或环境标志产品，依据品目清单和认证证书实施政府优先采购。优先采购的具体规定（如涉及） / 。
    2. 关于无线局域网认证产品政府采购清单中的产品，优先采购的具体规定（如涉及） 。

1. 确定中标候选人名单
   1. 采用综合评分法时，提供相同品牌产品（单一产品或核心产品品牌相同）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，评标委员会按照下述规定确定一个投标人获得中标人推荐资格，其他同品牌投标人不作为中标候选人。

□随机抽取

□其他方式，具体要求：\_\_\_\_\_

* 1. 采用综合评分法时，评标结果按评审后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并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。评分分值计算保留小数点后两位，第三位四舍五入。
  2. 采用最低评标价法时，评标结果按本章2.4、2.5调整后的投标报价由低到高顺序排列。投标报价相同的并列。投标文件满足招标文件全部实质性要求且投标报价最低的投标人为排名第一的中标候选人。
  3. 评标委员会要对评分汇总情况进行复核，特别是对排名第一的、报价最低的、投标或响应文件被认定为无效的情形进行重点复核。
  4. 评标委员会将根据各投标人的评标排序，依次推荐本项目（各采购包）的中标候选人，起草并签署评标报告。本项目（各采购包）评标委员会共（各）推荐 3 名中标候选人。

1. 报告违法行为
   1. 评标委员会在评标过程中发现投标人有行贿、提供虚假材料或者串通等违法行为时，有向采购人、采购代理机构或者有关部门报告的职责。
2. **评标标准**

采用综合评分法，满分为100分，由以下部分组成：

**第五包评分表如下：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **评分因素** | | **分值** | | **评分标准** |
| 1 | 商务  （10分） | 业绩  （6分） | | 6分 | 投标人自2021年1月1日（以合同签订时间为准）起至今承担类似项目业绩，每个业绩得1.5分，该项最高得6分（须提供合同首页、签字盖章页、合同关键内容页的复印件，并加盖投标人公章；合同乙方名称必须与投标人的名称完全一致，如公司名称发生变更，必须提供工商部门的证明文件，否则不得分） |
| 资质  （4分） | | 1分 | 投标人具有有效的信息安全管理体系认证证书的得1分，需提供证书复印件并加盖投标人公章，否则得0分。 |
| 1分 | 投标人具有有效的中国信息安全测评中心颁发的信息安全服务资质安全工程类证书的得1分，需提供证书复印件并加盖投标人公章，否则得0分。 |
| 1分 | 投标人具有有效的中国网络安全审查技术与认证中心颁发的信息安全服务资质认证证书（信息系统安全集成）三级（含）以上的得1分，需提供证书复印件并加盖投标人公章，否则得0分。 |
| 1分 | 投标人具有有效的中国网络安全审查技术与认证中心颁发的信息安全服务资质认证证书（信息安全应急处理）三级（含）以上的得1分，需提供证书复印件并加盖投标人公章，否则得0分。 |
| 2 | 技术服务（60分） | 需求理解分析  （5分） | | 5分 | 需求理解分析  █需求分析内容全面、详细具体、理解准确、重难点分析到位，紧贴我市广播电视网络视听安全监测态势感知，并能提出切实可行的解决办法，得5分；  █需求分析内容较全面，理解基本准确，贴我市广播电视网络视听安全监测态势感知，有一定的重难点分析和解决办法，得3分；  █需求分析内容为通用套话，或理解偏差较多，不贴实际业务需求，或未提到重难点分析，得1分；  █未提供需求理解与分析，得0分。 |
| 软件设计开发方案  （17分） | | 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.1资产管理**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.2等保管理**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.3安全监测**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.4攻击链分析**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.5深度融合分析**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.6网络攻防演练管理**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.7预警通报**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.8威胁情报**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.9全文检索**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **2.1网络安全数据分析管理**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **2.2行业网络信息安全分析引擎**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **3.1日志数据采集**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **3.2网络流量数据采集**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **3.3资产发现和采集**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **3.4漏洞数据采集设**计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **3.5安全事件数据采集**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （一）网行业网络安全监管（专网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **4数据存储**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 技术  参数  （15分）（**注：投标人需在采购需求偏离表中对技术要求的所有内容进行点对点应答，应在引用本招标文件的基础上，进行逐条逐项答复、说明或解释。漏报技术条款视为不满足。**） | 2分 | | 投标人应提供“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“二、货物需求一览表”中全部购置软硬件产品制造商授权书，并加盖原厂公章。  少提供1个产品制造商授权书的减1分，少提供2个及以上产品制造商授权书的减2分。 |
| 1分 | | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**1.流量探针（3G）**满足所有参数，得1分，有任一项不满足不得分。 |
| 1分 | | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**2.流量探针（1.7G）**满足所有参数，得1分，有任一项不满足不得分。 |
| 1分 | | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，3**.日志探针**满足所有参数，得1分，有任一项不满足不得分。 |
| 1分 | | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**4.Web应用防火墙系统（WAF）**满足所有参数，得1分，有任一项不满足不得分。 |
| 1分 | | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**5.漏洞探针**满足所有参数，得1分，有任一项不满足不得分。 |
| 1分 | | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**6.密码机**满足所有参数，得1分，有任一项不满足不得分。 |
| 1分 | | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**7.流量分流器**满足所有参数，得1分，有任一项不满足不得分。 |
| 1分 | | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**8.交换机（接入）（业务应用区接入交换机）**满足所有参数，得1分，有任一项不满足不得分。 |
| 1分 | | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**9.交换机（核心）**满足所有参数，得1分，有任一项不满足不得分。 |
| 1分 | | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**10.交换机（接入）（安全管理区接入交换机）**满足所有参数，得1分，有任一项不满足不得分。 |
| 1分 | | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**11.签名验签服务器**满足所有参数，得1分，有任一项不满足不得分。 |
| 1分 | | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**12.磁盘阵列**满足所有参数，得1分，有任一项不满足不得分。 |
| 1分 | | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**13.国密浏览器**满足所有参数，得1分，有任一项不满足不得分。 |
| 项目实施（9分） | 5分 | | 项目实施方案  █内容全面且描述详细具体可行，包括但不限于组织架构、进度计划、软件开发、安装实施、突发事件处置等，紧贴我市行业网络安全监测业务需求，针对性强，得5分；  █内容全面但描述细致度不够，能够包括组织架构、进度计划、软件开发、安装实施、突发事件处置等，贴近我市行业网络安全监测业务需求，有一定针对性，得3分；  █内容描述细为通用套话，内容缺项，不贴实际业务需求，缺乏针对性得1分；  █完全未描述或完全不具有针对性，得0分。 |
| 4分 | | 项目实施团队  █项目负责人  具有信息系统项目管理师（高级）资格证书且具有5年以上相关项目经验，得1分。需提供证书复印件、简历介绍及由投标人为其缴纳近3个月社保证明并加盖投标人公章，否则不得分。  █软件研发人员  具备CISP-CISD（注册信息安全开发人员）或CISP-DSG（注册数据安全治理专业人员）证书，且具备3年以上软件开发工作经验，每有一个证书得0.2分，最多得2分。需提供证书复印件、人员简历介绍及由投标人为其缴纳近3个月社保证明等材料，并加盖公章，否则不得分。同一人具备多个证书的，不重复计分。  █产品安装调试人员  具备CISAW（安全集成）或CISAW（安全运维）证书，且具备3年以上网络规划、设备安装、系统调试工作经验，每有一个证书得0.2分，最多得1分。需提供证书复印件、人员简历介绍及由投标人为其缴纳近3个月社保证明并加盖公章，否则不得分。同一人具备多个证书的，不重复计分。 |
| 质保期内服务（14分） | 5分 | | 质保期内服务方案  █内容全面且描述详细具体可行，包括但不限于组织架构、职责分工、业务运营、系统维护等，紧贴我市行业网络安全监测业务需求，针对性强，得5分；  █内容全面但描述细致度不够，能够包括组织架构、职责分工、业务运营、系统维护等，贴近我市行业网络安全监测业务需求，有一定针对性，得3分；  █内容描述细为通用套话，内容缺项，不贴实际业务需求，缺乏针对性得1分；  █完全未描述或完全不具有针对性，得0分。 |
| 5分 | | 质保期内应急预案  █内容全面且描述详细具体可行，包括但不限于组织架构、职责分工、设备抢修、应急处置等，紧贴我市行业网络安全监测业务需求，针对性强，得5分；  █内容全面但描述细致度不够，能够包括组织架构、职责分工、设备抢修、应急处置等，贴近我市行业网络安全监测业务需求，有一定针对性，得3分；  █内容描述细为通用套话，内容缺项，不贴实际业务需求，缺乏针对性得1分；  █完全未描述或完全不具有针对性，得0分。 |
| 2分 | | 投标人应提供“第五章采购需求 第五包 行业网络安全监测业务建设（专网端）”中“二、货物需求一览表”中全部软硬件产品开发商、制造商对本项目质保期内的售后服务承诺，并加盖投标人公章。  少提供1个产品售后服务承诺的减1分，少提供2个及以上产品售后服务承诺的减2分。 |
| 2分 | | 项目维护团队  具有CISP或CISAW证书，且具备2年以上网络安全项目运维工作经验，每有一个证书得0.5分，最多得2分。需提供证书复印件、人员简历介绍及由投标人为其缴纳近3个月社保证明并加盖公章，否则不得分。同一人具备多个证书的，不重复计分。 |
| 3 | 报价 | 投标报价 | 30分 | | 满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。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）×分值。  此处投标报价指经过报价修正，及因落实政府采购政策进行价格调整后的报价，详见第四章《评标方法和评标标准》2.4及2.5。 |

**第六包评分表准如下：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **评分因素** | | **分值** | **评分标准** |
| 1 | 商务  （10分） | 业绩  （6分） | 6分 | 投标人自2021年1月1日（以合同签订时间为准）起至今承担类似项目业绩，每个业绩得1.5分，该项最高得6分（须提供合同首页、签字盖章页、合同关键内容页的复印件，并加盖投标人公章；合同乙方名称必须与投标人的名称完全一致，如公司名称发生变更，必须提供工商部门的证明文件，否则不得分） |
| 资质  （4分） | 1分 | 投标人具有有效的信息安全管理体系认证证书的得1分，需提供证书复印件并加盖投标人公章，否则得0分。 |
| 1分 | 投标人具有有效的中国信息安全测评中心颁发的信息安全服务资质安全工程类证书的得1分，需提供证书复印件并加盖投标人公章，否则得0分。 |
| 1分 | 投标人具有有效的中国网络安全审查技术与认证中心颁发的信息安全服务资质认证证书（信息系统安全集成）三级（含）以上的得1分，需提供证书复印件并加盖投标人公章，否则得0分。 |
| 1分 | 投标人具有有效的中国网络安全审查技术与认证中心颁发的信息安全服务资质认证证书（信息安全应急处理）三级（含）以上的得1分，需提供证书复印件并加盖投标人公章，否则得0分。 |
| 2 | 技术服务（60分） | 需求理解分析（6分） | 6分 | 需求理解分析  █需求分析内容全面、详细具体、理解准确、重难点分析到位，紧贴我市广播电视网络视听安全监测态势感知，并能提出切实可行的解决办法，得6分；  █需求分析内容较全面，理解基本准确，贴我市广播电视网络视听安全监测态势感知，有一定的重难点分析和解决办法，得4分；  █需求分析内容为通用套话，或理解偏差较多，不贴实际业务需求，或未提到重难点分析，得2分；  █未提供需求理解与分析，得0分。 |
| 软件设计开发方案  （16分） | 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.1资产管理**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.2等保管理**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.3安全监测**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.4攻击链分析**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）知软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.5深度融合分析**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.6预警通报**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.7威胁情报**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **1.8全文检索**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **2.1网络安全数据分析管理**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **2.2行业网络信息安全分析引擎**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **3.1日志数据采集**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **3.2网络流量数据采集**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **3.3资产发现和采集**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **3.4漏洞数据采集设**计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **3.5安全事件数据采集**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 1分 | 针对招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”综合考虑投标人提供的软件设计开发方案是否全面、具体、内容是否详细且具有针对性、技术是否可行且具有先进性：  **4数据存储**设计开发方案：  全面且描述具体，具有针对性，得1分；  有一定的描述，但细致度不够或针对性不强，得0.5分；  完全未描述或完全不具有针对性，得0分。 |
| 技术  参数  （10分）（**注：投标人需在采购需求偏离表中对技术要求的所有内容进行点对点应答，应在引用本招标文件的基础上，进行逐条逐项答复、说明或解释。漏报技术条款视为不满足。**） | 2分 | 投标人应提供“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“二、货物需求一览表”中全部购置硬件产品制造商授权书，并加盖原厂公章。  少提供1个产品制造商授权书的减1分，少提供2个及以上产品制造商授权书的减2分。 |
| 2分 | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**1.流量探针（1.7G）**满足所有参数，得2分，有任一项不满足不得分。 |
| 2分 | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，2**.日志探针**满足所有参数，得2分，有任一项不满足不得分。 |
| 2分 | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**3.漏洞探针**满足所有参数，得2分，有任一项不满足不得分。 |
| 2分 | 投标人所投产品优于或完全满足招标文件“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“三、性能配置及技术指标要求 （二）软硬件设备，**4.流量分流器**满足所有参数，得2分，有任一项不满足不得分。 |
| 项目实施（10分） | 6分 | 项目实施方案  █内容全面且描述详细具体可行，包括但不限于组织架构、进度计划、软件开发、安装实施、突发事件处置等，紧贴我市行业网络安全监测业务需求，针对性强，得6分；  █内容全面但描述细致度不够，能够包括组织架构、进度计划、软件开发、安装实施、突发事件处置等，贴近我市行业网络安全监测业务需求，有一定针对性，得4分；  █内容描述细为通用套话，内容缺项，不贴实际业务需求，缺乏针对性得2分；  █完全未描述或完全不具有针对性，得0分。 |
| 4分 | 项目实施团队  █项目负责人  具有信息系统项目管理师（高级）资格证书且具有5年以上相关项目经验，得1分。需提供证书复印件、简历介绍及由投标人为其缴纳近3个月社保证明并加盖投标人公章，否则不得分。  █软件研发人员  具备CISP-CISD（注册信息安全开发人员）或CISP-DSG（注册数据安全治理专业人员）证书，且具备3年以上软件开发工作经验，每有一个证书得0.2分，最多得2分。需提供证书复印件、人员简历介绍及由投标人为其缴纳近3个月社保证明并加盖公章，否则不得分。同一人具备多个证书的，不重复计分。  █产品安装调试人员  具备CISAW（安全集成）或CISAW（安全运维）证书，且具备3年以上网络规划、设备安装、系统调试工作经验，每有一个证书得0.2分，最多得1分。需提供证书复印件、人员简历介绍及由投标人为其缴纳近3个月社保证明并加盖公章，否则不得分。同一人具备多个证书的，不重复计分。 |
| 质保期内服务（18分） | 6分 | 质保期内服务方案  █内容全面且描述详细具体可行，包括但不限于组织架构、职责分工、业务运营、系统维护等，紧贴我市行业网络安全监测业务需求，针对性强，得6分；  █内容全面但描述细致度不够，能够包括组织架构、职责分工、业务运营、系统维护等，贴近我市行业网络安全监测业务需求，有一定针对性，得4分；  █内容描述细为通用套话，内容缺项，不贴实际业务需求，缺乏针对性得2分；  █完全未描述或完全不具有针对性，得0分。 |
| 6分 | 质保期内应急预案  █内容全面且描述详细具体可行，包括但不限于组织架构、职责分工、设备抢修、应急处置等，紧贴我市行业网络安全监测业务需求，针对性强，得6分；  █内容全面但描述细致度不够，能够包括组织架构、职责分工、设备抢修、应急处置等，贴近我市行业网络安全监测业务需求，有一定针对性，得4分；  █内容描述细为通用套话，内容缺项，不贴实际业务需求，缺乏针对性得2分；  █完全未描述或完全不具有针对性，得0分。 |
| 2分 | 投标人应提供“第五章采购需求 第六包 行业网络安全监测业务建设（互联网端）”中“二、货物需求一览表”中全部软硬件产品开发商、制造商对本项目质保期内的售后服务承诺，并加盖投标人公章。  少提供1个产品售后服务承诺的减1分，少提供2个及以上产品售后服务承诺的减2分。 |
| 4分 | 项目维护团队  具有CISP或CISAW证书，且具备2年以上网络安全项目运维工作经验，每有一个证书得1分，最多得4分。需提供证书复印件、人员简历介绍及由投标人为其缴纳近3个月社保证明并加盖公章，否则不得分。同一人具备多个证书的，不重复计分。 |
| 3 | 报价 | 投标报价 | 30分 | 满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。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）×分值。  此处投标报价指经过报价修正，及因落实政府采购政策进行价格调整后的报价，详见第四章《评标方法和评标标准》2.4及2.5。 |

1. **采购需求**

**第五包** **行业网络安全监测业务建设（专网端）**

**采购需求**

**注：**招标文件带有“★”号条款为实质性条款，不满足要求为**无效投标。**

# 概述

网络视听新媒体综合监管平台升级改造项目（以下简称“本项目”）按照北京市广播电视和网络视听行业的全流程、全要素、综合监管要求，对网络全方位管理，实现网络视听监管、网络视听舆情监管、行业网络安全监管等业务需要。一是实现网络视听内容监测、网络宣传、节目审核、精品创作、机构管理、综合业态管理等业务，为北京市网络视听行业统筹管理提供数据依据及分析建议。二是进行网络视听舆情监管，围绕北京广播电视和网络视听行业进行舆情监测及预警，实现对广电舆情的全面监测和风险预警。三是提供行业网络安全监管服务，对广电播控网络进行全面监测，掌握关键网络运行状况和安全风险，有针对性地研判预警，提升行业整体安全水平。

升级改造后的系统将扩充网络视听内容监管业务范围、提升网络视听舆情监管能力、增设行业网络安全监管能力，以及遵循集成化、一体化、数据化、网络化、智能化原则构建为各类应用提供共性服务的公共业务应用组件、数据存储分析等支撑环境，并根据等保三级要求构建相关网络安全环境。

本包实现对本市22家播出传输单位业务系统的网络安全监测，进行风险识别、威胁发现、安全事件实时告警及可视化展示等安全防护，保障播出安全、网络安全。

网络视听监管、网络视听舆情监管业务部署在北京市政务云，通过专用通信链路和软件平台相连；网络安全监测前端部署在14个区融媒体中心、北京新媒体集团等22家播出单位，行业网络安全监测业务（专网端）软件平台部署在北京市广播电视监测中心指定机房，探针等前端设备部署在各安播单位。

★本包所有具有互联网协议地址规划方式的设备软硬件均须支持 IPv6互联网协议。

★本包软件开发及部署须根据采购人要求适配相应数据库、操作系统、服务器等信创产品。

★本包软件开发需符合网络安全等级保护2.0三级防护要求。

★投标人需配合本项目第一包、第二包、第七包，做好：①智能运维、数据底座、指挥调度、数据可视化展示的数据对接及相关开发工作；②做好单点登录~~的~~协议接口开发工作；③提供完整业务流闭环方案，做好通过北京安播PC端、北京安播移动端、短信途径向各安播单位发送告警信息、事件信息、通报信息及接收各安播单位上报信息等业务的数据对接及相关开发工作，具备信息反馈渠道，各安播单位可通过北京安播PC端、北京安播移动端完成事件查看、处置、反馈、事件消除等动作。投标人提供承诺函，格式自拟，加盖公章。

# 采购需求一览表

## 行业网络安全监管（专网端）软件开发需求一览表

各部分功能需求见“三、性能配置及技术指标要求 （一）行业网络安全监管（专网端）软件开发”

| **序号** | **名称** | | **数量** | **单位** | **备注** |
| --- | --- | --- | --- | --- | --- |
| 1 | 业务应用 | 资产管理 | 1 | 套 |  |
| 2 | 等保管理 | 1 | 套 |
| 3 | 安全监测 | 1 | 套 |
| 4 | 攻击链分析 | 1 | 套 |
| 5 | 深度融合分析 | 1 | 套 |
| 6 | 网络攻防演练 | 1 | 套 |
| 7 | 预警通报 | 1 | 套 |
| 8 | 威胁情报 | 1 | 套 |
| 9 | 全文检索 | 1 | 套 |
| 10 | 数据分析 | 网络安全数据分析管理 | 1 | 套 |
| 11 | 网络信息安全分析引擎 | 1 | 套 |
| 12 | 数据采集 | 日志数据采集 | 1 | 套 |
| 13 | 网络流量数据采集 | 1 | 套 |
| 14 | 资产发现和采集 | 1 | 套 |
| 15 | 漏洞数据采集 | 1 | 套 |
| 16 | 安全事件数据采集 | 1 | 套 |
| 17 | 数据存储 | 数据存储 | 1 | 套 |

## 软硬件设备需求一览表

性能配置及技术指标要求见“三、性能配置及技术指标要求 （二）软硬件设备”。

| **序号** | **设备名称** | **数量** | **单位** | **备注** |
| --- | --- | --- | --- | --- |
| 1 | 流量探针 | 1 | 台 | 流量探针（3G） |
| 2 | 流量探针 | 25 | 台 | 流量探针（1.7G） |
| 3 | 日志探针 | 25 | 台 | 日志探针 |
| 4 | Web应用防火墙系统（WAF） | 2 | 台 | Web应用防火墙系统 |
| 5 | 漏洞探针 | 1 | 台 | 漏洞探针 |
| 6 | 密码机 | 2 | 台 | 服务器密码机 |
| 7 | 流量分流器 | 25 | 台 | 流量分流器 |
| 8 | 交换机（接入） | 2 | 台 | 业务应用区接入交换机 |
| 9 | 交换机（核心） | 2 | 台 | 核心交换机 |
| 10 | 交换机（接入） | 2 | 台 | 安全管理区接入交换机 |
| 11 | 签名验签服务器 | 1 | 台 | 签名验签服务器 |
| 12 | 磁盘阵列 | 1 | 台 | 备份存储 |
| 13 | 国密浏览器 | 530 | 套 | 国密浏览器 |

**注：以上表（一）中序号1至序号17和表（二）中序号13，合计预算控制金额为：211.025万元，超出按无效处理；**

**表（二）中序号1至序号12预算控制金额为：630.296172万元，超出按无效处理。**

# 性能配置及技术指标要求

## 行业网络安全监管（专网端）软件开发

#### 业务应用

##### 资产管理

###### 资产概况

* + - 1. 资产动态检测识别

1. 具备按照单位、系统、网站、设备、软件、服务、机房、网络、数据库维度对资产数据分类及展示，具备增删改查、导入导出、批量处理等功能；
2. 具备漏洞扫描报告导入功能，类型包括主机漏洞、配置核查、WEB漏洞、弱口令等，文件格式支持xml和excel；支持对导入后的漏洞扫描报告进行管理，内容包括报告名称、报告类型、资产脆弱性数量、报告文件格式、解析模板、导入时间等；支持报告下载功能；
3. 具备对资产的脆弱性评估功能，实现资产潜在漏洞发现和管理，通过对已纳管资产数据与漏洞知识库关联匹配生成潜在漏洞信息，资产潜在漏洞信息包括资产名称、资产类型、版本型号、所属单位、首次发现时间，以资产视角展示潜在漏洞信息；
4. 具备漏洞库知识库，包括漏洞发布时间、漏洞名称、漏洞类型、危害等级、漏洞编号、CNNVD编号、CNVD编号、其他编号、漏洞来源、威胁类型等信息，支持漏洞详情查看功能。
   * + 1. 总体资产状况统计
5. 具备对各安播单位资产统计功能，包括资产数量情况（单位数量统计、网站/系统数量统计、软件数量统计、设备数量统计和IP数量统计）、资产运营情况、资产重要程度统计、硬件资产分布情况、软件资产分布情况、系统资产分布情况、单位资产分布情况；以TOP10形式进行展示；
6. 具备资产数据展示功能，包括柱状图、环状图、矩形树图等形式。

###### 资产归档

* + - 1. 资产归档模板管理

具备资产归档模板管理能力，支持不同类型资产的导入模板，包括单位、设备、系统、网站、软件、机房等资产类型模板。

* + - 1. 资产数据导入、统计、展示配置

1. 具备将填报数据按模板分类导入功能，支持展示导入结果信息，包括正常导入的资产数据、无法导入的资产数据，模板中填报数据能自动解析存入对应的数据存储结构中；
2. 具备资产导入结果统计及展示能力，对已填报单位数量及填报的数据进行统计及展示。

###### 一键搜索

* + - 1. 资产分类规则配置

具备资产分类规则配置功能，通过预置规则自动将原始发现的资产进入纳管状态，对资产的归属规则、运营规则和忽略规则进行配置。

* + - 1. 资产状况时间设置检索

1. 通过关键字方式，从单位、设备、软件、服务、系统、网站、机房、网络、数据库、用户等维度，对资产进行精确检索或模糊检索，能够点击查看具体资产的详情信息；
2. 具备与、或、非等常见查询语法示例；
3. 具备通过语法规则组合对资产数据进行高级检索；
4. 具备高级筛选功能，通过关联资产、资产状态、更新时间、资产数据范围、时间范围等维度对资产进行筛选；
5. 具备历史检索记录管理功能，能够查看历史检索的资产数据范围、时间范围、检索语句等内容，历史记录不少于10条；
6. 具备将检索条件保存至“常用检索”功能，支持对“常用检索”条件的查看、选择、删除等操作。

###### 资产融合

* + - 1. 资产自动纳管规则配置

1. 建立资产纳管规则，包括资产归属规则、资产运营规则，自动将监测前端采集、手动录入的待纳管资产进行统一管理；支持对资产纳管规则的启用、停用等配置操作；
2. 资产归属规则：通过探针序列号、IP、域名等信息确定资产归属单位；
3. 资产运营规则：通过IP、MAC等信息自动发现资产冲突；建立置信度规则自动解决资产冲突；
4. 具备资产审核功能，对纳管规则输出的结果进行人工审核，包括新增资产、更新资产、忽略资产。
   * + 1. 资产融合规则配置

具备资产融合规则功能，支持基于IP、所属单位、端口、协议等维度对各前端采集的原始资产数据进行自动融合，过滤重复或无效资产数据。

##### 等保管理

###### 定级备案管理

1. 具备手动录入及模板导入等保备案信息功能，包括系统等保备案、单位等保备案两个维度。
2. 系统等保备案内容包括系统名称、系统类型、保护等级、备案单位、距离复测截止日期、备案时间、备案状态、整改情况等，支持系统备案数据的编辑、删除、导出、详情查看等操作。
3. 单位等保备案内容包括单位基本信息、已备案系统、未备案系统等，支持单位备案数据的编辑、删除、导出、详情查看等操作。

###### 等保数据统计

1. 具备行业等保工作总体情况统计功能，包括行业各级系统数量、各安播单位各级系统数量、测评情况（复测、复测逾期）、检查情况、限期整改情况和系统安全状况等；
2. 具备系统测评逾期告警功能，针对各安播单位等保系统到期未开展等保测评情况进行告警；
3. 系统测评逾期告警推送至中心平台，由中心平台对接监测中心现有短信发布模块、北京安播移动端发布平台及北京安播PC端，发布至各安播单位；
4. 具备统计结果展示功能，以柱状图、表格等形式进行展示；
5. 具备安播单位等保工作详情查看功能，包括系统数量、系统名称、备案等级、测评开展情况、整改情况、责任人与联系方式等信息。

###### 检查任务管理

1. 具备等保检查任务管理功能，支持等保检查任务的创建、编辑、删除、导出、查询等操作，指派指定人员对等保单位开展检查工作；
2. 具备等保检查任务阶段管理功能，包括创建、检查、处置、反馈、归档等阶段；
3. 具备按照安播单位、等保系统等维度对检查任务进行统计功能，内容包括等保检查项、等保检查要点、检查要点合格情况等；支持按照时间范围对检查统计结果进行筛选。

###### 测评信息管理

1. 具备备案系统测评信息管理功能，支持上传测评报告、测评合同、测评计划等文档；支持对系统测评结果信息的编辑、导入、导出、删除、查询、详情等操作；
2. 具备备案系统测评信息展示功能，包括系统名称、测评状态、测评时间、测评机构、测评师、测评分值、测评结果等内容；
3. 具备测评机构信息管理功能，支持对测评机构信息的编辑、导入、导出、删除、查询、详情等操作；
4. 具备测评机构信息展示功能，内容包括测评机构、服务范围、服务级别、有效期、地址、联系人、联系方式、传真等；
5. 具备测评师信息管理功能，支持对测评师信息的编辑、导入、导出、删除、查询、详情等操作；
6. 具备测评师信息展示功能，内容包括姓名、所在机构、从业时间、证书编号、证书级别、联系方式等。

###### 等保综合分析报表

1. 具备对各安播单位等保情况综合分析报表报告功能，报表支持以文字、表格、饼状图、柱状图等方式展示行业网络安全等级保护工作整体情况，具备报表报告预览功能；
2. 具备报表报告数据源管理功能，支持自定义数据源的来源渠道，包括本地文件、数据库的数据表等；
3. 具备报表报告数据集管理、数据目录权限设定功能，实现不同角色的访问权限控制；
4. 具备报表报告导出功能，文件格式包括Excel、Word、PDF等类型；报告周期包括年报、月报等，时间可自定义。

##### 安全监测

###### 告警管理

* + - 1. 威胁告警数据管理

1. 具备告警信息展示功能，对系统发现的各类网络安全告警实时展示；
2. 具备告警处置状态记录功能，通过不同底纹颜色等方式区别告警状态处置与否；
3. 具备告警信息管理功能，支持告警信息导入、导出、批量打标签等操作，告警标签可自定义：
4. 支持对告警状态变更操作，状态包括无需处置、误报、查实需处置、已处置、IP封禁等，支持逐个操作及批量操作；
5. 具备告警统计功能，按照单位名称、时间范围、告警类型等维度对告警信息进行统计；
6. 具备告警查询功能，按照单位名称、时间范围、告警类型等维度对告警信息进行查询；
7. 具备展示历史告警查询条件记录功能，包括查询范围、时间范围、查询语句等内容，能够选择历史查询条件再次查询；
8. 支持告警信息字段配置，支持按特定字段排序；具备以柱状图、折线图等形式展示指定时间、不同类型、不同等级告警功能；
9. 支持查看告警详情，包括告警基本信息（告警类型、攻击源IP、受害者IP、告警级别等）、关联的规则信息、原始告警列表等。
   * + 1. 高级威胁创建分析联动
10. 具备对选定的高级威胁告警信息创建研判任务；
11. 一键转入研判任务，通过攻击频次、访问关系、原始告警实现威胁分析的联动处置能力。

###### 事件管理

* + - 1. 事件关联分析管理

1. 具备网络安全事件生成功能，支持网络安全告警生成事件、人工添加事件等方式；事件字段包括事件标题、事件分类、事件标签列表、事件等级、上报单位、事件描述、发现时间、事发单位、事态发展概述及初判原因、响应处置要求、处置建议等内容；
2. 具备网络安全事件管理功能，包括事件审核、处置、查询、导出等操作。审核结果包括通过、不通过、无需处置；事件处置类型包括启动事件通报、启动应急、关联应急、无需处置等；事件查询支持时间范围、关键字、事件等级、事件标题、事件分类、处置状态、上报单位等维度查询；
3. 具备网络安全事件详情查看功能，包括事件基本信息、关联信息、举证信息、要素信息、处置进展、操作记录、补充信息等内容。
   * + 1. 威胁多维度综合评估分析
4. 具备网络安全事件分类分级功能，事件分类包括恶意程序事件、网络攻击事件、数据安全事件、信息内容安全事件、违规操作事件、设备设施故障事件、安全隐患事件、异常行为事件、其他事件等内容；事件分级包括一般事件、较大事件、重大事件和特别重大事件等；
5. 具备网络安全事件全流程管理功能，包括事件待提交、待研判、被退回、待处置、处置中、已处置等；
6. 具备网络安全事件展示功能，包括列表视图、单列视图等方式。

###### 数据分析

* + - 1. 多维数据分析

具备多维数据分析功能，通过汇聚网络安全告警数据、网络安全事件数据，分析北京市广播电视行业安全趋势、威胁同比/环比情况，得出安播单位系统资产告警排名、情报命中情况、攻击源TOP排名等内容。

* + - 1. 图形化统计分析

具备图形化展示功能，通过柱状图、环状图、曲线图、表格等方式对分析结果进行展示。

###### 监测规则管理

* + - 1. 监测规则配置管理

1. 具备告警监测规则库，内容包括有害程序、攻击利用、信息破坏、内容安全、拒绝服务、异常活动、信息收集、安全隐患、可用性、后渗透行为等威胁的识别规则；
2. 具备告警监测规则与攻击链模型各阶段映射功能；
3. 具备告警监测规则统一管理功能，包括规则新增、编辑、复制、删除、启动、导入、导出、详情、查询等。其中，规则启动包括测试启动、正式启动；规则查询包括规则名、规则来源、模板类型、数据源、规则阶段、规则状态、攻击方向、防护实体信息、规则标签、任务状态等查询条件；
4. 具备告警监测规则展示功能，支持规则字段配置。
   * + 1. 数据字段关联配置
5. 具备对采集的网络安全原始数据关联配置功能，利用监测规则中等于、包含等条件组合，将原始数据字段与告警数据字段建立关联，实现网络安全原始数据过滤、告警自动确认、告警归并、告警基本信息字段的重新定义；
6. 具备对告警基本信息字段的自定义功能，将网络安全原始数据字段（包括源IP、目的IP、源端口、目的端口等）映射为告警基本信息字段（包括攻击源IP、受害者IP、源端口、目的端口等）。

###### 资源对象管理

1. 具备安播单位资源对象库，内容包括安播单位资产IP地址、端口、时间等资源；
2. 设计告警监测规则可直接引用安播单位资源对象库内相关资源；
3. 具备资源对象统一管理功能，包括资源对象新增、编辑、复制、删除、导入、导出、详情、查询等。

###### 行业模型配置

1. 具备广电行业规则配置功能，包括新建规则、命中规则、告警生成策略、告警归并策略等；新建规则时，支持自定义规则名称、规则版本、发布时间、规则状态、规则模板、规则描述、规则标签、规则属性等内容；
2. 通过广电行业规则组合生成网络安全告警监测模型，包括：网络攻击监测模型、应用威胁监测模型、运维管理监测模型、异常行为监测模型等；
3. 具备监测模型筛选功能，基于规则名称、数据源、任务状态、标签等多种条件对模型进行筛选。

###### 数据统一检索

* + - 1. 数据字段关联关系配置

具备字段关联关系配置功能，通过语法规则（and、or等）对告警基本信息字段进行组合，实现流量日志、网络日志数据精准查询。

* + - 1. 数据统一分析检索

1. 具备统一分析检索功能，通过关键字对流量日志、网络日志数据进行模糊检索；
2. 具备检索结果展示功能，包括日志数据检索条数、日志数量时间分布、单条日志信息详情等；
3. 具备日志检索结果导出功能。

##### 攻击链分析

###### 资产画像

1. 具备资产画像功能，通过资产管理模块中的基础信息、所属安全域、关联资产、漏洞信息、变更记录等维度对安播单位资产进行画像；
2. 具备安播单位资产关联功能，关联维度包括：资产组成、拓扑结构、关键要素等，为威胁告警信息富化提供数据支撑；
3. 基于安全设备、计算设备、网络设备、终端设备等资产要素构建拓扑结构；
4. 具备资产漏洞影响范围评估功能，通过漏洞的基本信息、影响资产信息评估漏洞对业务系统的影响范围。

###### 攻击者同源分析

1. 具备攻击者同源分析功能，通过识别攻击者IP信息，归并同源IP，将属于同一攻击者的相关网络威胁进行关联、归并；
2. 具备攻击者同源分析任务管理功能，包括任务创建、概览、编辑、复制、删除等功能；
3. 具备分析任务工作台，包括数据汇聚、数据过滤、高危IP清单、攻击者画像等功能；
4. 数据汇聚：收集安全事件信息；
5. 数据过滤：通过添加可信IP或无需处置IP，过滤无效告警；
6. 高危IP清单：列表展示待处置的高危攻击者IP信息，内容包括攻击时间、告警数据来源、源IP、今日攻击次数、攻击/告警类型、告警名称、告警状态、攻击结果、受害者信息等；
7. 攻击者画像：提供攻击者IP关联告警信息补充功能，包括告警信息补录、画像信息补录等方式，形成完整的攻击者画像；
8. 具备攻击者同源分析结果展示功能，以图谱、地图、表格等方式，展示每个攻击IP的累计攻击次数、IP库标签、IP溯源信息及IP历史画像信息等内容；

###### 攻击链标签建模

具备攻击链标签建模功能，结合安播单位业务系统实际情况，设置恶意程序入侵链条、网络攻击链条的识别场景，对告警所属ATT&CK攻击链不同阶段打标签。

###### 基于钻石模型分析

1. 具备攻击总览视图，攻击链包括侦查跟踪、武器构建、载荷投递、突防利用、安装植入、通信控制、达成目标等阶段；
2. 展示每个阶段的全量告警数据；
3. 以时间轴方式展示攻击过程；
4. 支持调整告警所属的攻击链阶段；
5. 具备钻石模型分析展示功能，展示威胁相关的攻击者、受害者、基础设施和能力维度的详细信息。

##### 深度融合分析

###### 失陷情报数据匹配

1. 系统具备自动接收各监测前端日志探针、流量探针采集的安播单位业务系统网络安全数据功能；
2. 具备失陷情报数据匹配功能，通过威胁情报（威胁情报的定义详见1.9.3 威胁情报模型配置）与实际资产的比对，发现失陷资产，威胁情报包括：恶意IP地址、恶意URL、恶意DNS、恶意Email、MD5等。

###### 失陷数据编码映射

1. 具备对监测前端采集的流量数据、日志数据预处理能力，提供输入类、编码类、富化类、输出类、控制类等插件，创建数据自动处理流程，提高数据预处理工作效率；数据预处理工作包括数据质量评估、数据清理、数据集成、数据转换、数据标记等；
2. 具备数据预处理任务配置功能，任务支持引用一个或多个数据自动处理流本开展数据预处理工作；
3. 具备数据预处理任务管理功能，包括新增、运行、停止、重启、编辑、删除等；
4. 具备数据预处理任务展示功能，包括任务名称、状态、处理日志速度等；
5. 具备未解析数据当前日志、历史日志的下载、查看功能。

###### 数据归一化管理

1. 具备对各监测前端采集数据归一化管理功能，对各安播单位资产的异构日志格式进行归一化处理；
2. 对采集和处理过的安全数据进行存储，包括结构化数据、半结构化数据和非结构化数据存储；其中，对日志数据、告警信息可设置存储天数；
3. 归一化后的网络安全数据及相关日志、报告等信息全部推送至本项目数据底座治理、存储，完成相应适配工作。

###### 规则关联分析

1. 具备关联规则分析功能，通过日志、情报、资产等类型数据进行关联，发现恶意代码、异常行为等安全威胁并进行告警；
2. 具备关联分析规则管理功能，包括规则新增、编辑、分类、查询、导入、导出、删除、详情等；
3. 提供统计类、序列类、关联类规则模板库，以图形化处理的方式编排规则模型。

###### 智能模型分析

具备广电行业网络安全智能分析模型，根据各安播单位业务系统实际场景，分析采集到的网络安全数据资源，通过关联分析规则自动匹配，对发现的安全威胁进行告警，包括Web攻击、网络攻击、异常行为发现等安全威胁。

##### 网络攻防演练

###### 单位管理

1. 具备手动录入/批量导入攻防演练单位数据；
2. 具备演练单位管理功能，支持添加、删除、编辑等操作；
3. 具备演练单位信息展示功能，内容包括：名称、简称、组织机构代码、单位类型、行业类别、网站URL、上级主管、地址、标签、描述等。

###### 人员管理

1. 具备手工录入/批量导入攻防演练人员数据；
2. 具备演练人员管理功能，支持添加、删除、编辑等操作，支持人员调配；
3. 具备演练人员信息展示功能，内容包括姓名、所属单位、分类、技能标签、身份证号、联系电话、手机号码、联系邮箱等。

###### 装备管理

1. 具备演练装备物资信息管理功能，支持导入、导出、批量删除、编辑等操作；
2. 具备装备物资信息展示功能，内容包括名称、分类、所属单位、版本、技能标签、描述等。

###### 手段管理

1. 具备攻防演练应急技术手段管理功能，支持创建、删除、编辑等操作；
2. 具备应急技术手段信息展示功能，内容包括手段名称、手段模板、手段类型、标签、描述。

###### 1.6.5.综合管理

1. 具备报告上传功能，导入攻防演练期间产生的攻击报告、防守报告、总结报告等；
2. 具备报告统计功能，按照攻防双方、单位名称、年度等维度统计相关报告；
3. 具备报告导出功能，支持按照单位名称、年度、攻防双方等维度导出，支持WORD、WPS、PDF等格式；
4. 具备成绩录入功能，按照单位名称、年度、得分情况进行录入；
5. 具备成绩统计功能，包括年度、单位名称、攻防双方等进行统计、展示。

###### 1.6.6.问题管理

1. 具备网络攻防演练发现问题的导入功能，与事件关联分析管理模块对接，通过人工添加事件、模板导入事件等方式导入攻防演练发现的问题；
2. 具备网络攻防演练发现问题的统计分析功能，包括单位名称、年度、问题类型、问题数量等维度；
3. 具备网络攻防演练发现问题的导出功能，支持按照单位名称、年度、问题类型等维度导出，支持WORD、WPS、PDF等格式；
4. 具备网络攻防演练发现问题的展示功能，通过图表、折线图、柱状图等方式展示，维度包括各安播单位历年发现问题数量、每类问题历年数量等；
5. 具备网络攻防演练发现问题的通报、追踪功能，通过与专项通报分析管理模块对接，实现对攻防演练发现问题的下发及整改追踪。

##### 预警通报

将安全监测模块中监测分析产生的网站漏洞、风险和事件及手工导入的外部获取的安全事件等数据，通过日常通报、专项通报等方式，及时通报涉事的单位，督促涉事单位进行快速处置，确保问题得到及时整改、反馈、核实、归档，从而实现完整业务流程的闭环。

###### 安全事件维度分析

1. 具备安全事件日常通报发起功能，对通过研判确认的安全事件，一键发起通报；并可手动创建通报；
2. 日常监测告警生成的网络安全事件，推送至中心平台，由中心平台对接监测中心现有短信发布模块、北京安播移动端发布平台及北京安播PC端，发布至各安播单位；其中，通过北京安播移动端发布平台及北京安播PC端下发的网络安全事件信息，可携带多种类型附件；
3. 具备安全事件展示功能，通过接入事件管理模块的数据，以连线图、表格等方式展示待通报的安全事件信息和数量。

###### 日常通报分析管理

1. 具备通报事件分析功能，分析通报反馈数量、整改平均完成时间等；
2. 具备日常通报任务统计功能；能够对通报反馈情况、问题整改情况、事件处罚情况进行统计；
3. 具备日常通报任务管理功能，支持按照模板自动生成网络安全隐患告知书、事件报告；
4. 具备日常通报处置流程展示功能，流程状态包括未处置、处置中和处置完毕等；展示内容包括处置单位、处置状态、处置时间、延期状态等；
5. 具备日常通报反馈功能，支持各安播单位通过北京安播PC端上传整改报告，实现业务流程闭环处置；
6. 具备整改报告统计功能，支持按照时间、单位名称、事件类型等维度统计、检索、上传、下载整改报告；

###### 专项通报分析管理

1. 具备针对特定风险、特定事件制定专项通报任务，基于上级单位通报的网络安全风险、漏洞隐患等网络安全信息，通报各安播单位进行风险排查；
2. 专线通报任务信息推送至中心平台，由中心平台对接监测中心现有短信发布模块、北京安播移动端发布平台及北京安播PC端，发布至各安播单位；其中，通过北京安播移动端发布平台及北京安播PC端下发的专线通报任务信息，可携带多种类型附件；
3. 针对同一通报任务，具备手动添加或按组分配多个对象，并一键下发功能；
4. 具备专项通报任务配置功能，配置对象包括：通报标题、通报下发时间、通报下发单位、通报内容、风险种类、初判风险等级、初判风险类型、通报状态、处置完成时间等，并支持添加多种类型附件、多个附件功能；
5. 具备自动生成专项通报任务报告功能，报告内容包括：任务类型、任务对象、任务执行时间、任务执行结果等；
6. 具备专项通报任务报告统计功能，支持按照时间、单位名称、事件类型等维度统计、检索、上传、下载专项通报任务报告。

###### 通报事件统计

具备通报事件统计功能，按时间范围对通报事件类型、单位被通报次数、受影响资源、通报整改工作阶段、超时未反馈、被通报事件来源、被通报单位问题严重情况等维度进行统计。

###### 综合通报管理

1. 具备综合报告生成功能，支持按照时间、单位名称、系统名称、通报事件类型等维度，综合统计分析日常通报、专项通报事件，自动生成综合通报报告；
2. 提供综合报告模板管理，内容包括通报类型、通报编号、通报标题、通报基本情况（事件类型、涉事IP等、事件描述、单位名称等)、通报处理意见等；
3. 具备报告模板新建、编辑、配置、删除、检索、启用等功能；
4. 具备综合报告内容预览、编辑、导出功能，格式支持Word、PDF等。

###### 通报规则配置管理

1. 具备通报流程模板管理功能，支持对日常通报、专项通报任务的业务流程进行管理，包括创建、编辑、复制、删除等内容；
2. 具备通报流程模板编排功能，支持配置审核、重新提交、签收、执行、验证、归档等各环节，对各环节的执行时限、执行人范围、表单配置、可见范围、操作选项和消息模板进行配置；
3. 具备各类通报流程模板展示功能，以列表方式展示通报流程，包括通报类型名称、类型描述、更新时间等内容；
4. 具备通报流程模板调用功能，支持在新建日常通报、专项通报任务时选择对应的模板发起通报任务。

##### 威胁情报

###### 事件深度分析引擎

1. 具备事件深度分析引擎，利用引擎内的威胁情报库与告警管理模块产生的告警攻击源IP进行比对，实现攻击源IP详细信息富化；
2. 具备黑客属性识别功能，包括：所属组织、威胁名称、威胁类型、威胁级别、地理位置信息等；
3. 具备黑客信息识别功能，包括：攻击IP、告警类型、源MAC地址、攻击次数、载荷长度、载荷内容等；
4. 具备黑客能力识别功能，包括：攻击手段、关联资产等；
5. 具备同源攻击IP分析功能，通过引擎筛查的条件组合，实现对全量告警的同源攻击IP识别、告警；
6. 具备根据已知特征进行告警降噪功能，已知特征包括：受害IP（IP 段）、攻击源IP（IP 段）、威胁情报、威胁名称、域名、目的端口、源IP（IP段）、目的IP（IP段）等信息的降噪。

###### APT活动拓展分析

1. 具备对APT事件分析功能，通过探针采集的攻击原始日志、原始告警对APT攻击事件所处阶段（侦察、入侵、命令控制、横向渗透、目的执行、痕迹清理）进行分析；
2. 以折线图等形式对APT攻击事件所处阶段进行展示。

###### 威胁情报模型配置

1. 具备手动、自动更新威胁情报库功能；
2. 支持第三方威胁情报导入，情报格式包括JSON格式 、STIX格式、XLSX格式、OPENIOC格式等；
3. 具备威胁情报分析模型配置功能，通过匹配IP、域名、MD5等信息，创建威胁情报分析规则。
4. 具备ATT&CK知识库，可将安全告警与ATT&CK知识库进行比对，展示告警所采用的攻击技术详情。

##### 全文检索

###### 分布式数据索引

对流量探针、日志探针采集到的全部日志创建索引，索引条件包括时间维度、日志类型等，提升系统检索速度。

###### 高级汇聚数据分类查询

具备对日志文件内容的查询功能；

1. 对不同格式（Unicode编码、UTF8编码、URL解码/编码、Hex解码/编码、Base64解码/编码、进制转换等）日志进行归一化处理、入库、统一展示；
2. 具备快捷查询功能，通过关键字查询日志内容；
3. 具备高级查询功能，通过等于、包含、不等于等语法组合，创建自定义查询条件，精确查询日志内容；
4. 具备日志查询结果详情展示功能，能够查看结果字段及对应值；
5. 具备历史查询记录管理功能，能够查看历史检索的日志查询范围、时间范围、查询语句等内容，历史记录不少于10条；
6. 具备将查询条件保存至“常用查询”功能，支持对“常用查询”条件的查看、选择、删除等操作。

#### 安全数据采集

##### 日志数据采集

1. 对接日志探针，通过SYSLOG、HTTP等协议自动接收日志探针采集到的各安播单位资产的日志信息，日志探针的采集方式包括 Syslog、SNMP Trap、文本格式、数据库、Netflow、HTTP等。
2. 具备日志探针管理功能，能够查看全部日志探针的详细信息，包括各探针接收的日志总数、解析日志总数、未解析日志总数等。

##### 网络流量数据采集

1. 对接流量探针，通过kafka等协议自动接收流量探针采集到的各安播单位流量信息，流量探针通过旁路镜像等方式，采集各安播单位关键系统在IPv4/IPv6双协议栈下的全部流量；
2. 具备流量探针管理功能，能够查看全部流量探针的详细信息，包括探针上传流量、平台接收流量、差值率等。

##### 资产发现与采集

具备安播单位资产数据自动获取、手动录入功能；

1. 对接探针，通过kafka等协议自动接收采集识别安播单位关键系统内的IP地址、MAC地址等信息，实现资产的自动获取；
2. 具备手动录入、模板导入安播单位关键系统的资产信息功能；包括资产名称、厂家、型号、IP地址、网络掩码、MAC地址等信息。

##### 漏洞数据采集

对接漏扫探针，通过接口对接等方式自动接收漏扫探针采集到的各安播单位关键系统的漏洞信息。

##### 安全事件数据采集

对接北京广播电视台、歌华有线公司的态势感知系统，通过接口对接等方式自动获取该系统生成的安全事件信息。

#### 安全数据处理

1. 按照采购人统一要求进行数据标准化处理，存储入库；
2. 具备数据处理流程管理功能，以可视化拖拽等方式设计数据处理流程，包括流程创建、删除、导入、输出统计、查看、编辑、复制等功能；
3. 具备对采集到的网络安全数据进行富化处理的能力，包括字段映射、归一化数据、静态值映射、动态数据映射、字段删除、地理位置映射、字段改名、默认值填充、系统时间填充、数组拆解、RedisKV富化、日志打标、字典表等映射、字典表IP号段富化、字段加工映射等；

#### 安全数据存储

1. 具备结构化、半结构化和非结构化数据存储功能，分类构建资产库、脆弱性库、情报库、用户库、知识库、基础库、对象库、原始库等，并集中配置管理；
2. 具备配置数据重要程度、存储天数等功能。

#### 安全数据分析

##### 网络安全数据分析管理

###### 规则关联分析

具备关联分析规则设计功能，通过过滤、关联统计、序列、基线日志统计、基线行为统计等基础模型，设计贴合广电业务场景的关联分析模型，包括有害程序、攻击利用、信息破坏、内容安全、拒绝服务、异常活动、信息收集、安全隐患、可用性、后渗透行为等模型；提供模型数量不少于700个。

###### 攻击面安全分析（资产安全分析）

1. 具备资产安全分析功能，将已知的特定漏洞，与漏扫探针识别出的各安播单位资产漏洞信息进行比对，筛查各安播单位业务系统是否存在该漏洞；
2. 关联预警通报模块，将筛查出的漏洞信息通知相关单位。

###### 高级威胁分析

具备高级威胁分析功能，将流量探针采集到的流量，与威胁情报模块中的威胁情报进行比对，调用样本分析引擎，筛查恶意文件，实现对恶意程序执行、恶意代码投递等伪装攻击的检测。

###### 漏洞分析

1. 具备漏洞知识库，包括公共漏洞信息、自定义漏洞信息；
2. 具备手动、自动更新漏洞知识库功能；
3. 具备漏洞分析功能，将漏洞探针采集到的漏洞信息与漏洞知识库进行匹配，识别漏洞的危害等级、类型，并进行告警；
4. 具备漏洞统计功能，按照漏洞危害等级、受影响资产数量、漏洞类型等维度统计各安播单位资产漏洞情况；
5. 具备漏洞查询功能，按照单位名称、漏洞名称、漏洞类型、漏洞危害等级等维度查询漏洞情况；
6. 具备漏洞展示功能，以表格、柱状图等方式展示各安播单位资产漏洞情况。

###### 异常行为分析

1. 构建异常行为分析模型，包括特殊端口关闭/启用模型、域名周期性解析模型、跳板机行为模型、资产异常外连模型、暴力破解模型等异常行为模型；
2. 将流量探针采集到的流量数据与异常行为模型进行比对，对发现的异常行为进行告警。

###### WebShell攻击分析

1. 构建Webshell攻击分析模型，具备识别asp、php、jsp、cgi等网页文件构建的WEBshell攻击的能力；
2. 将流量探针采集到的流量数据与Webshell攻击分析模型进行比对，对发现的WEBshell攻击行为进行告警；
3. 具备Webshell分析内容展示功能，包括WebShell利用工具名称、攻击方向、源IP、目的IP、目的端口、目的单位、目的资产名称，通过趋势图呈现Webshell攻击的活跃度。

###### 弱口令分析

1. 构建弱口令分析模型，具备弱口令资产发现能力；
2. 将流量探针采集到的流量数据与弱口令分析模型进行比对，对发现的弱口令登录行为进行告警；
3. 具备弱口令统计功能，按照单位名称、资产名称等维度统计弱口令情况。

###### 代理隧道分析

1. 构建代理隧道分析模型，具备frp端口转发、reDuh隧道代理、reGeorg隧道代理、Tunna隧道代理等事件发现能力；
2. 将流量探针采集到的流量数据与代理隧道分析模型进行比对，对发现的代理隧道事件进行告警。

##### 网络信息安全分析引擎

###### 流量检测分析引擎

结合流量探针实现以下功能：

1. 提供流量检测分析引擎，对网络链路全流量采集、全数据分析，具备网络异常行为感知能力、多维数据索引能力、网络攻击定位与取证能力；
2. 具备告警攻击研判能力，利用双向检测机制、原始数据包和研判模型，对攻击结果进行判断，结果包括：攻击尝试、攻击成功；
3. 支持对应用层协议进行攻击检测，包括HTTP、FTP、TFTP、TLS、SSH、SMB、DNS、NFS、DHCP、SNMP等；
4. 支持对多种攻击类型进行检测，包括：漏洞利用检测、各类特征检测、恶意攻击程序检测、拒绝服务攻击检测、可疑通信检测。

###### 关联分析引擎

1. 具备关联分析引擎，根据规则关联分析（5.1.1）设计的分析模型，创建关联分析任务，生成告警、归并告警，产生安全分析结果数据，并进行告警；
2. 具备关联分析模型筛选功能，按照规则名、规则来源、模板类型、数据源、规则阶段、规则状态、攻击方向、规则标签、任务状态等条件对模型进行筛选。

###### 资产分析引擎

1. 具备资产分析引擎，利用引擎内的资产特征库与资产发现与采集模块发现的资产信息进行匹配，实现资产的精确识别；
2. 构建资产关系图谱，展示各安播单位业务系统的设备图谱。

###### 样本分析引擎

通过接收各种格式的文件，结合静态检测，动态检测和威胁情报检测技术，对恶意文件进行识别并进行告警。

1. 具备样本分析引擎，对执行文件、脚本类文件、多媒体文件、文档类文件、压缩文件等文件样本进行分析，识别恶意文件；
2. 将流量探针采集到的文件、手动上传的文件与样本分析引擎进行比对筛查，对发现的恶意文件进行告警；
3. 具备筛查结果展示功能，包括恶意文件的MD5、文件类型、文件名、检测结果、检测时间、检测状态等信息；
4. 支持恶意文件和筛查报告下载、批量下载。

###### ATT&CK分析引擎

具备ATT&CK分析引擎，对ATT&CK知识库进行手动、自动更新；

具备视图展示功能，将系统发现的各类网络告警与ATT&CK模型各阶段进行映射，展示各阶段的告警数量。

###### 情报分析引擎

1. 具备威胁情报统计功能，统计内置威胁情报、自定义情报的数量；
2. 具备威胁情报查询功能，可对告警信息携带的恶意IP地址、恶意URL、文件MD5等信息进行查询，确认告警威胁程度；
3. 具备威胁情报展示功能，以表格形式展示威胁情报信息。

###### APT分析引擎

1. 具备APT事件识别功能，利用探针采集的恶意文件MD5、DNS流量、TCP流量、UDP流量等信息，与事件深度分析引擎内的威胁情报库进行比对，识别APT攻击事件，并进行告警；
2. 具备APT分析引擎，联动流量探针查看原始数据包中特征告警详情，内容包括：源目IP、情报类型、攻击类型、攻击结果、告警级别等信息。

## 软硬件设备

### 1.流量探针（3G）

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 硬件要求 | 标准机架式设备；冗余电源；千兆电口≥6个，千兆光口≥4个，万兆光口≥2个，管理网口≥1个；接口扩展板卡插槽≥1个；USB接口≥2个。 |
| 2 | 性能要求 | 网络流量的实时接收采集（多路）≥3Gbps（具备网络流量采集、威胁数据采集和日志上报功能）；并发请求数≥400万；最大新建连接数≥15万/秒；具备流量数据、威胁数据进行采集、还原、解密、外发等能力，支持不少于19种协议还原能力。 |
| 3 | 部署方式 | 支持通过流量镜像的方式获取核心交换机网络流量，实现网络流量数据采集、威胁检测和日志外发，支持通过重置会话的方式阻断TCP威胁会话连接，支持通过流量被动识别资产。 |
| 4 | 离线采集 | 具备离线采集功能，通过手动Pcap导入方式对离线流量进行采集，支持批量导入，支持流量回放。 |
| 5 | 协议解析 | 具有自定义解析流量能力，支持基于正则表达式、固定长度等提取模式对应用流量解析。支持基于全部会话流的攻击检测功能，无漏报。 |
| 6 | 协议采集 | 支持采集和分析的协议包括：HTTP、FTP、TFTP、SMTP、TLS、SSH、IMAP、SMB、DNS、NFS、DHCP、SNMP、SIP、RDP等。  具备加密流量协议解析能力，能够分析镜像加密流量，确保发现安播单位系统终端、服务器、虚拟机等违规外联、数据外发泄露等行为，无漏报。 |
| 7 | 协议还原 | 具备还原多种文件传输协议能力，包括：Web（HTTP）、FTP、SMB等。 |
| 8 | 威胁检测 | 检测常见的溢出攻击、跨站脚本、SLQ注入、拒绝服务、跨站请求伪造、目录遍历、webshell上传等。 |
| 9 | 具备攻击检测能力的扩展功能，支持自定义恶意文件、自定义漏洞、自定义间谍软件、自定义威胁情报等。 |
| 10 | 具备间谍软件检测能力，检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、隧道、代理通道、后门程序、远控木马等。 |
| 11 | 支持对检测的告警事件结合检测机制、原始数据包和研判模型等规则进行深层次研判，给出告警事件的攻击结果。 |
| 12 | 告警过滤 | 具备攻击告警的过滤能力，能够针对IP地址或端口对攻击告警进行过滤，支持攻击特征高亮展示。 |
| 13 | 本地情报 | 本地集成威胁情报库，支持基于威胁情报的失陷主机和挖矿主机检测，情报数量≥100万条。 |
| 14 | 加密协议解析 | 具备基于SSL协议的SMTPS、POP3S、IMAPS、HTTPS流量解密功能。 |

### 2.流量探针（1.7G）

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 硬件要求 | 标准机架式设备，冗余电源，千兆电口≥6个，千兆光口≥2个万兆光口≥2个，Console口≥1个，接口扩展板卡插槽≥2个。 |
| 2 | 性能要求 | 同时开启网络流量采集、威胁数据采集和日志上报功能情况下混合流吞吐量≥1.7Gbps，HTTP并发连接数≥300万，HTTP新建连接速率≥2万/秒；具备流量数据、威胁数据进行采集、还原、解密、外发等能力，支持不少于19种协议还原能力。 |
| 3 | 部署方式 | 支持通过流量镜像的方式获取核心交换机网络流量，实现网络流量数据采集、威胁检测和日志外发，支持通过重置会话的方式阻断TCP威胁会话连接，支持通过流量被动识别资产。 |
| 4 | 离线采集 | 具备离线采集功能，通过手动Pcap导入方式对离线流量进行采集，支持批量导入，支持流量回放。 |
| 5 | 协议解析 | 具有自定义解析流量能力，支持基于正则表达式、固定长度等提取模式对应用流量解析。支持基于全部会话流的攻击检测功能，无漏报。 |
| 6 | 协议采集 | 支持采集和分析的协议包括：HTTP、FTP、TFTP、SMTP、TLS、SSH、IMAP、SMB、DNS、NFS、DHCP、SNMP、SIP、RDP等。  具备加密流量协议解析能力，能够分析镜像加密流量，确保发现安播单位系统终端、服务器、虚拟机等违规外联、数据外发泄露等行为，无漏报。 |
| 7 | 协议还原 | 具备还原多种文件传输协议能力，包括：Web（HTTP）、FTP、SMB等。 |
| 8 | 威胁检测 | 检测常见的溢出攻击、跨站脚本、SLQ注入、拒绝服务、跨站请求伪造、目录遍历、webshell上传等。 |
| 9 | 具备攻击检测能力的扩展功能，支持自定义恶意文件、自定义漏洞、自定义间谍软件、自定义威胁情报等。 |
| 10 | 具备间谍软件检测能力，检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、隧道、代理通道、后门程序、远控木马等。 |
| 11 | 支持对检测的告警事件结合检测机制、原始数据包和研判模型等规则进行深层次研判，给出告警事件的攻击结果。 |
| 12 | 告警过滤 | 具备攻击告警的过滤能力，能够针对IP地址或端口对攻击告警进行过滤，支持攻击特征高亮展示。 |
| 13 | 本地情报 | 本地集成威胁情报库，支持基于威胁情报的失陷主机和挖矿主机检测，情报数量≥100万条。 |
| 14 | 加密协议解析 | 具备基于SSL协议的SMTPS、POP3S、IMAPS、HTTPS流量解密功能。 |

### 3.日志探针

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 硬件要求 | 标准机架式设备，内存容量≥16GB，硬盘容量≥4TB，千兆电口≥6个，千兆光口≥4个，扩展插槽≥2个。 |
| 2 | 性能要求 | 日志采集处理能力≥2500EPS，最大日志源≥150个，本次不少于35个日志源授权。 |
| 3 | 采集方式 | 具备Syslog、SNMP Trap、JDBC、FTP、SFTP等协议的日志采集能力，采集网络设备、安全设备、主机及业务系统等资产日志；具备通过规则对各类日志归一化、过滤、合并、富化的能力。 |
| 4 | 资产信息 | 具备对所采集资产的信息管理功能，包括名称、类型、厂商、序列号、IP/MAC、地理位置、联系人等信息。 |
| 5 | 日志展示 | 具备对所采集资产的运行时长、日志源数量、关联事件数、告警总数、已保存日志时长、存储空间等情况展示功能。 |
| 6 | 事件搜索 | 具备自定义“事件查询条件”功能，支持多条件组合查询并保存为策略功能，支持对不同场景的自定义策略查询。 |
| 7 | 归一化 | 具备日志归一化功能，实现对多元异构日志格式进行统一描述和处理。 |
| 8 | 资产管理 | 支持自定义资产类型及资产属性；支持对资产打标签，支持对标签内容进行查询和管理。 |
| 9 | 解析字段 | 日志解析内置不少于60个字段，属性字段可扩展，可根据审计需要自行创建字段，内置及新增的所有字段均可参与事件查询、关联分析和报表数据源统计。 |
| 10 | 关联分析 | 支持展示日志属性之间的聚合关系，支持手动选择日志属性，支持属性调整，具备显示多维事件分析图功能。 |
| 11 | 安全分析场景 | 支持多种安全分析场景，包括恶意代码、可疑控制、入侵利用、违规行为、嗅探行为、关联审计等。 |

### 4.Web应用防火墙系统（WAF）

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 硬件要求 | 标准机架式设备，冗余电源，10/100/1000M Base-TX≥8个，千兆SFP插槽≥8个，万兆光口≥4个，扩展槽≥6个。 |
| 2 | 性能要求 | 网络吞吐量≥12G，HTTP吞吐量≥10G，应用层并发连接数≥700万，web安全保护站点数量不限制。支持对HTTP或HTTPS的Web攻击行为进行分析并拦截。 |
| 3 | 部署模式 | 具备旁路部署、单臂模式、透明模式、代理模式，支持旁路镜像流量分析功能。 |
| 4 | 信息隐藏 | 具备隐藏服务器信息功能，支持自定义错误页面返回码、错误页面标题、错误页面内容以及重定向URL功能。 |
| 5 | 攻击防护 | 具备识别和阻断攻击行为功能，包括SQL注入、XSS跨站攻击、PHP反序列化防护、Cookie防护等。 |
| 6 | 蜜罐防御 | 具备轻量级蜜罐防御功能。 |
| 7 | 安全防御 | 具备Web业务加固防御功能，提供行为识别、弱密码检测、会话安全、CGI安全、跨站请求伪造以及业务流程控制的防御功能。 |
| 8 | 机器学习 | 具备机器学习引擎，支持语义防护等深度学习防护功能，实现SQL复杂语义攻击的识别和学习。 |
| 9 | 源区域访问控制 | 具备地域访问控制功能，支持根据国家、城市等元素进行地域访问控制，并可自定义区域控制。 |
| 10 | 合规检测 | 具备协议合规检测功能，可根据实际网络状况自定义协议参数合规标准，过滤非法数据。 |
| 11 | 敏感信息防护 | 具备敏感信息检测防护功能，对服务器信息、错误页面信息等进行防护。 |
| 12 | 协议识别 | 具备协议识别及解码能力，支持URL解码、XML解码、JSON解析、Base64解码、Unicode解码、十六进制转换，支持解析7层以上混合编解码能力。 |

### 5.漏洞探针

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 硬件要求 | 标准机架式设备，10/100/1000M Base-TX≥6个，千兆光口≥4个，扩展槽≥2个，USB接口≥2个，具备显示面板；内存容量≥32G，硬盘容量≥1TB。 |
| 2 | 性能要求 | 并发任务数≥10个，单任务支持扫描IP数≥150个，支持IP地址数量≥1024个，网页扫描并发任务数≥7个域名（具备网页并发扫描能力），具备系统漏洞检测、web漏洞检测、数据库漏洞检测、配置合规检测、弱口令检测等检测功能。 |
| 3 | 扫描任务 | 具备系统扫描、Web扫描、弱口令扫描分析功能，支持对指定IP地址段多种扫描任务一键下发功能。 |
| 4 | 扫描策略 | 支持立即扫描、定时扫描、周期性扫描、断点续扫等扫描任务执行方式。 |
| 5 | 分析报告 | 根据系统漏洞、Web漏洞、弱口令扫描结果自动生成分析报告。 |
| 6 | 扫描模式 | 具备标准扫描、快速扫描、完全扫描、深度扫描等扫描模式。 |
| 7 | 漏洞特征库 | 覆盖CNVD、CNNVD等多种漏洞标准。特征库漏洞数不少于40万个，支持手动更新、在线更新。 |
| 8 | 统计视图 | 具备不同维度的统计视图，包括系统情况、WEB应用情况、风险分布等。 |
| 9 | 检测类型 | 支持扫描通用操作系统、交换路由设备、安全设备、物联网设备、虚拟化、中间件、国产操作系统、国产数据库、国产办公软件、WEB网站、虚拟化软件及大数据组件。 |
| 10 | 资产管理 | 支持资产信息管理，含资产名称、IP、MAC、负责人等。 |

### 6.密码机

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 硬件要求 | 标准机架式设备，CPU≥8核，主频≥2.3GHz，内存≥16G，硬盘≥120G SSD存储，10/100/1000Mbps自适应网口≥2个，Console口≥1个，USB口≥2个，冗余电源。 |
| 2 | 性能要求 | SM4加解密性能≥860Mbps；SM3杂凑性能≥400Mbps；SM2密钥对生产性能≥16000对/秒；SM2签名性能≥12000次/秒；MAC\_SM4≥885Mbps；最大并发连接数≥5100。 |
| 3 | 功能要求 | 支持对称加密/解密功能，支持分组加密，支持ECB、CBC、OFB、CFB、CTR、XTS、CCM等模式。 |
| 4 | 三级密钥结构 | 三级密钥结构，具备系统保护密钥对生成的密钥进行加密，生成密钥对会话密钥加密功能。 |
| 5 | 数据信封 | 支持基于RSA/SM2密码算法的数字信封功能，支持由内部密钥保护到外部密钥保护的数字信封转换功能。 |
| 6 | 密钥备份 | 支持内部密钥的安全备份和恢复。 |
| 7 | 密钥存储 | 支持对称密钥、RSA密钥和SM2密钥的加密存储。 |
| 8 | 随机数生成芯片 | 随机数发生器应采用国家密码管理主管部门批准的物理噪声源芯片,应提供多路随机源,至少采用两个独立的物理噪声源芯片实现。 |
| 9 | 访问控制 | 具备白名单访问控制功能，支持增加单个或网段IP。 |
| 10 | 密钥管理 | 具备生成、存储、使用、导入、下载、删除等密钥管理功能。 |
| 11 | 日志管理 | 具备日志记录功能，具备以 syslog 方式发送日志功能，具备日志审计功能。 |
| 12 | 日志对接 | 支持与日志审计系统对接，对日志审计系统审计过的日志进行加密，满足密评要求。 |
| 13 | 三权管理 | 采用三权分立的模式，配置系统管理员、安全管理员、安全审计员。管理员和操作员身份通过智能密码钥匙进行双因子认证。 |
| 14 | 高可用 | 具备双机主备、集群模式。 |

### 7.流量分流器

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 设备要求 | 配置48个10/100/1000BASE-T以太网端口，4个万兆SFP+接口  交换容量≥2.4Tbps/24Tbps，包转发率≥552Mpps/762Mpps 交流电源模块×2，风扇插×2个 MAC地址条目≥320K |
| 2 | 功能要求 | 支持 MAC 认证、802.1x 认证、Portal 认证 |
| 3 | 支持IGMP v1/v2/v3； |
| 4 | 支持SNMP v1/v2/v3、Telnet； |
| 5 | 支持VxLAN二层、三层网关，支持三层路由功能 |
| 6 | ★支持IPV6； |
| 7 | 配齐光模块 |

### 8.交换机（接入）（业务应用区接入交换机）

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 设备要求 | 配置48个10GE SFP+端口，8个100GE QSFP28端口  交换容量≥4.8Tbps，包转发率≥2000Mpps 交流电源模块≥2，模块化风扇≥2 |
| 2 | 功能要求 | 支持 MAC 认证、802.1x 认证、Portal 认证 |
| 3 | 支持IGMP v1/v2/v3； |
| 4 | 支持SNMP v1/v2/v3、Telnet； |
| 5 | 支持VxLAN二层、三层网关，支持三层路由功能 |
| 6 | ★支持IPV6； |
| 7 | 配齐光模块 |

### 9.交换机（核心）

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 设备要求 | 配置2个主控处理单元，2个交换网单元  配置1块48端口十兆/百兆/千兆以太网电+4端口万兆以太网光端口（SFP+）接口板，1块48端口万兆以太网光接口板(SFP+)  交换容量≥430Tbps，转发性能≥172800Mpps  交流电源模块≥2，模块化风扇≥2  主控槽位≥2，业务槽位≥6 |
| 2 | 功能要求 | 具备设备状态监控功能，能集中监控各类板卡、风扇、电源等模块 |
| 3 | 支持 MAC 认证、802.1x 认证、Portal 认证 |
| 4 | 支持IGMP v1/v2/v3； |
| 5 | 支持SNMP v1/v2/v3、Telnet； |
| 6 | 支持VxLAN二层、三层网关，支持三层路由功能 |
| 7 | ★支持IPV6； |
| 8 | 配齐光模块 |

### 10.交换机（接入）（安全管理区接入交换机）

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 设备要求 | 配置24个10/100/1000BASE-T以太网端口，4个万兆SFP+接口 交换容量≥432Gbps，包转发率≥155Mpps 交流电源模块≥2，模块化风扇≥2 |
| 2 | 功能要求 | 支持 MAC 认证、802.1x 认证、Portal 认证 |
| 3 | 支持IGMP v1/v2/v3； |
| 4 | 支持SNMP v1/v2/v3、Telnet； |
| 5 | 支持三层路由功能 |
| 6 | ★支持IPV6； |
| 7 | 配齐光模块 |
| 8 | 支持集群或堆叠技术 |

### 11.签名验签服务器

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 硬件要求 | 标准机架式设备，CPU≥8核，主频≥2.3GHz，内存≥16G，硬盘≥120G SSD，10/100/1000Mbps自适应网口≥2个，Console口≥1个，USB口≥2个，冗余电源。 |
| 2 | 性能要求 | SM2签名/验签(tps)≥12000/6000，RSA 2048签名/验签(tps)≥1640/11790，RSA 1024签名/验签(tps)≥4650/11766，SM3杂凑算法速率≥400Mbps，SM1算法加/解密速率≥850Mbps，SM4算法加/解密速率≥860Mbps，MAC≥880Mbps，最大并发连接数≥5100。 |
| 3 | 签名验签 | 支持基于SM2算法的PKCS#1、PKCS#7 Attached、P7 Detached签名/验证功能。 |
| 4 | 密钥存储 | 支持对称密钥、RSA密钥和SM2密钥的加密存储。 |
| 5 | 密钥安全 | 支持内部密钥的安全备份和恢复。 |
| 6 | 访问控制 | 支持IP白名单、连接口令等访问控制功能。 |
| 7 | 管理功能 | 支持SNMP协议，支持通过SYSLOG服务外发业务日志功能，支持NTP时间同步功能。 |
| 8 | 数据信封 | 支持基于RSA/SM2密码算法的数字信封功能，数字信封格式符合PKCS#7、GM/T0010等标准中定义的数据类型。 |
| 9 | 多信任域支持 | 支持配置不同的证书信任域，支持配置不验证、根证书、CRL、OCSP等多种验证策略。 |
| 10 | 证书管理 | 支持证书链管理功能，支持配置多个CA或者多级CA，可同时配置多条证书链。 |
| 11 | 支持国密SM2和RSA算法证书申请、导入、查询、删除、下载、存储功能。 |

### 12.磁盘阵列

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 设备要求 | 标准机架式设备，  CPU为多核多处理器，处理器数量≥2颗，每颗处理器核心数≥24核，主频≥2.6GHz；  内存≥128GB  磁盘槽位≥12个，3.5寸SAS、SATA磁盘接口  缓存≥16GB；  8TB 3.5寸硬盘≥12块，  千兆以太网口≥4个；  万兆以太网光端口（SFP+）≥4个，配齐光模块；  电源模块≥2个；  支持RAID1,5,6,10,50,60,热备模式；  PCIE扩展插槽≥3个。 |
| 2 | 功能要求 | 至少具备X86/虚拟机/云主机的整机快照功能、持续数据保护功能、P2P/V/C整机迁移功能、分钟级业务恢复重建功能、数据去重与合并功能、多级恢复验证功能，可选无系统X86/虚拟机/云主机裸机、WindowsSever、linux还原代理功能；可选虚拟化灾备验证/演练系统功能。 |
| 3 | 支持数据重删去重功能；支持文件验证功能模块，支持虚拟化验证主机功能；配置自动化驱动适配功能模块；支持后台非固定密钥功能； |
| 4 | 支持备份时通过灾备系统进行网络带宽占用限速、磁盘读写占用限速，以确保备份时对生产的影响小并且在可控范围内； |
| 5 | 支持顺序IO的磁盘数据块复制技术，无需对数据类型、逻辑以及关联性解析，无需磁盘指针反复寻求备份数据。 |
| 6 | 支持拓展CDP持续数据保护功能，可拓展提供物理主机、虚拟化主机、超融合主机、云主机提供CDP持续数据保护，实时备份磁盘任意时刻的状态，备份时间粒度最小可达微秒级，实现RPO趋近于0 |
| 7 | 网络可配置“网卡自动关闭/定时开启策略”，还可将除备份数据传输端口外的SSH、网络访问等网络端口全部关闭。 |
| 8 | 可在灾备系统的Web控制台上为目标机做各种必要的配置（差异硬件驱动配置、系统IP/路由配置和脚本配置），实现任意品牌/技术的服务器、虚拟机和云主机之间的异构自动化灾难重建。 |
| 9 | 支持拓展整机全场景恢复，无需部署配置操作系统、应用和数据库等系统环境，实现全场景带业务逻辑的整机灾难重建，无需人工手动安装驱动、更改注册表信息、应用配置信息等。 |
| 10 | 支持拓展快速恢复重建功能，在千兆网络环境中，无需预置灾备演练或灾难恢复环境，无论数据量大小。 |
| 11 | 源主机和异构目标机（物理机、虚拟机和云主机）灾难重建时自动完成适配驱动兼容适配。 |
| 12 | 支持以图形或WEB方式进行批量操作管理。 |

### 13.国密浏览器

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 基础要求 | 适配信创、Windows平台的网络版浏览器客户端。提供不少于530套授权，含三年国密功能激活授权。 |
| 2 | 功能要求 | 浏览器的内核不低于Blink102版本； 浏览器的V8引擎版本不低于10.2.0.0。 |
| 3 | 提供查看源代码功能，可查看网页源代码；提供开发者工具，支持网页调试能力，包括：网页元素查看和修改，控制台输入输出，源代码查看和调试，网络请求分析，性能分析等。 |
| 4 | 可设定在指定时间、浏览器退出时或每天首次启动时自动清除上网痕迹：包含浏览记录，下载记录，Cookie及其它网站数据，页面缓存，保存的密码和其他登录数据，自动填充表单数据。 |
| 5 | 支持本地用户数据加密，防止保存的密码被明文导出。敏感类数据支持绑定设备加密，只能本机使用，非敏感不绑定设备加密。 |
| 6 | 支持IE内核，以兼容老旧应用。支持自动切换内核，双核无缝传递cookies数据。 |
| 7 | 具备显示所有连接管控平台的浏览器客户端总数、活跃用户数、应用数量和可信网站数，点击可显示详细信息。 |
| 8 | 支持开启/关闭客户端登录功能，支持配置客户端登录方式， |
| 9 | 具备管理员新建受信站点，包含支持\*通配符和对可信站点进行编辑、删除。按模板填写后上传可批量添加受信任站点。 |
| 10 | 支持统一配置下发非国密网址，客户端访问策略网址时，对于支持国密、非国密双协议的网址，强制使用非国密协议建立通信 |

# 售后服务要求

投标人应提供详细的项目《需求理解分析》《软件设计开发方案》《项目实施方案》《质保期内服务方案》《质保期内应急预案》。

**（一）需求理解分析**

投标人应提供详细的《需求理解分析》，要求内容全面、详细具体、理解准确、重难点分析到位，紧贴我市广播电视网络视听安全监测态势感知，并能提出切实可行的解决办法。

**（二）软件设计开发方案**

投标人应按照采购需求，制定详细的软件开发设计方案，包括软件功能需求分析、系统总体架构设计、代码编写、测试和上线部署调试、系统联调、软件测评、验收等内容及计划安排，提供设计说明书、设计图等材料。

配合本项目的第三方软件测评机构做好中心平台软件测评、安全测评并按要求进行相应整改。

**（三）项目实施方案**

投标人应提供详细的《项目实施方案》。内容包括：组织架构、进度计划、软件开发、安装实施、突发事件处置等内容。

投标人应遵守北京市及采购人有关规定，主动配合监管平台项目其他建设单位、软件测评、安全测评单位、密码应用评估单位、监理单位的工作。

合同签订后，60个自然日内，完成购置软硬件设备交货；合同签订后，180个自然日内，完成软件研发、部署、调试等工作。

投标人应参与本项目数据标准化方案制定工作，提供网络安全监测业务专业意见。

投标人应配合第一包做好数据可视化相关工作。

★项目实施过程中，采购人根据业务工作实际情况，可对本项目业务功能需求进行深化设计，中标人应配合采购人进行设计方案、软件开发的调整，功能达到采购人要求。投标人提供承诺函，格式自拟，加盖公章。

中标人负责协调各安播单位安装探针等前端设备。

**（四）项目实施团队**

投标人应为本项目实施配备专门的项目技术团队，包括项目负责人、软件研发人员、产品安装调试人员等，负责本项目中心平台软件开发、产品安装调试和布线等具体实施工作。

项目实施团队中，软件研发人员不少于10名，进行行业网络安全监管软件开发研发设计；产品安装调试人员不少于5名，进行软硬件设备安装调试。项目负责人具有5年以上相关项目经验，具备软件开发、网络规划、系统调试能力，具备信息系统项目管理师（高级）资格证书；软件研发人员需具备3年以上软件开发工作经验，具备CISP-CISD（注册信息安全开发人员）或CISP-DSG（注册数据安全治理专业人员）证书；产品安装调试人员需具备3年以上网络规划、设备安装、系统调试工作经验，具备CISAW（安全集成）或CISAW（安全运维）证书；团队人员需提供人员简历等材料。

软件研发人员、设备安装调试人员的交通、食宿等费用由投标人承担，且技应遵守采购人现场的各项规章制度和安全操作规程，并服从采购人管理。

**（五）培训**

投标人免费提供设备原理、操作使用、维护等培训，项目验收前提供1次培训，质保期内每年1 次。

**（六）质保期内服务**

投标人应提供本项目质量保证期内的详细服务方案、应急预案。应设有热线服务电话，当出现突发事故事件时，采购人在任何时候可以得到及时响应和事故事件及时处置。

**1. 运行维护**

投标人应提供《质保期内服务方案》，内容包括：组织架构、职责分工、业务运营、系统维护等，内容应详细具体、可行且具有针对性，确保业务顺畅开展，确保系统稳定运行。

质保期内应当按照采购人的要求，每月至少进行1次巡检维护，安全播出重要保障期、重要安全检查前进行专项巡检，满足广播电视安全播出工作要求。

（1）运行维护内容

运行维护内容应当包括但不限于：

检查维护软硬件设备运行状态、日志；备份数据、日志；检查维护病毒库、规则库等软件运行和版本升级更新情况，保持当前版本最新；资产梳理、安全策略优化、故障排除等，保障监管平台网络安全、稳定运行。

（2）运行维护报告

运行维护报告包括：内容概述、设备软硬件主要指标及运行状态、日志情况、故障现象及处理、软件更新情况、规则库更新、策略调优、维护日期以及维护人员签字等内容。

每次维护工作完成，应向采购人提交维护报告。

**2.维护团队**

本项目质量保证期内，投标人应提供网络安全专业维护团队，专门负责监管平台网络安全运维保障工作，应明确维护团队成员职责任务。质量保证期内维护团队成员相对稳定，人员数量不少于4人，应具备CISP或CISAW证书及2年以上网络安全项目运维工作经验。

维护人员应遵守采购人各项规章制度、安全操作规程等相关规定，并服从采购人管理，配合采购人做好网络安全保障有关工作。

**3. 应急处置**

投标人应提供《质保期内应急预案》，内容包括：组织架构、职责分工、设备抢修、应急处置等，详细具体可行且具有针对性的，确保网络安全突发事件事故得到及时有效处置，保障平台安全稳定运行。

投标人应提供7×24小时专人电话支持服务，出现网络安全事件事故时，30分钟内响应，4小时内到达故障现场，备用设备板卡或部件在8个小时内送达现场。故障处理完成后，应急处置人员应向采购人提交应急处置情况报告。

应急处置人员到达现场后，即使不是合同中的设备出现故障（含软件系统故障），投标人有责任帮助或协同采购人查找问题所在，并帮助采购人解决问题。

**★4. 现场技术支持（**投标人提供承诺函，格式自拟，加盖公章**）**

（1）广播电视安全播出重要保障期（元旦、春节、两会、十一等），按照采购人要求，投标人安排1名技术人员现场值守服务，处置突发故障，保障平台安全稳定运行。

（2）质量保证期内，投标人应安排3名网络安全专业技术人员提供5×8小时驻场技术服务。人员要求具有CISP或CISAW等网络安全资质证书，主要工作为协助做好网络安全运营，分析网络安全告警，处置网络安全事故事件，维护软硬件设备确保其正常运行，编写相关技术材料等。

（3）技术人员提供现场技术支持服务的交通、食宿等费用由中标人承担，且技术人员应遵守采购人现场的各项规章制度和安全操作规程，并服从采购人管理。

**5. 备品备件**

投标人应备有充足的备品备件，能为采购人提供7×24小时优质、迅速、及时的备品备件技术支持，不能由于备品备件等不足而影响监管平台安全稳定运行。

投标人提供详细的备品备件清单。

**五、交货**

交货时间：购置软硬件设备，合同签订后60个自然日内；

研发软件，合同签订后180个自然日内。

交货地点：北京市广播电视监测中心指定地点。

**六、试运行**

软件研发部署、设备安装、系统调试等工作完成后，且整体项目达到初验标准后，本包进行初验，投入试运行；试运行期不少于180个自然日，试运行期出现的问题全部解决后，申请项目验收。

**七、验收**

本项目验收条件为：

1.研发软件、购置软硬件设备全部到货并符合采购要求；

2.按要求完成设备安装、策略部署、调试等工作；

3.设备试运行期满并且出现的问题全部解决；

4.项目文档资料齐全并符合要求；

5.配合测评机构完成本项目的软件测评、网络安全等级保护三级的测评、密码应用评估，并对测评和评估不合格项完成整改。

上述5个条件全部满足后，北京市广播电视监测中心组织专家依据项目合同和国家行业标准及相关规定，对项目进行验收。

**八、质量保证**

投标人应承诺提供的货物是全新的、未使用过的，并符合招标文件要求及投标文件技术描述中规定的质量、规格和性能要求。

★本项目所有货物质量保证期为：自项目通过终验之日起2年。

**九、知识产权**

投标人必须为本项目提供满足需要的所有软、硬件使用授权许可，如若发生侵犯知识产权、专利权、所有权、版权或软件正版化等行为时，其侵权责任与采购人无关，由投标人承担相应的责任，并不得损害采购人的利益。

本项目所开发软件的著作权在内的全部知识产权归采购人所有，软件开发完成后，中标人须将软件开发的所有成果，包括设计文档、用户文档、数据库设计文档、软件源代码、软件运行程序、安装使用手册等全部交付采购人。

**十、廉政要求**

投标人和采购人承诺共同加强廉洁自律、反对商业贿赂。

1. 投标人不向采购人工作人员行贿或馈赠礼金、有价证券、贵重礼品；
2. 投标人不报销应由采购人或工作人员支付的费用；
3. 投标人不向采购人工作人员支付劳务报酬；不安排采购人工作人员参加宴请及娱乐活动。

**十一、采购标的所属行业**

本项目采购标的属于《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）中的：工业。

**第六包 行业网络安全监测业务建设（互联网端）**

**采购需求**

**注：**招标文件带有“★”号条款为实质性条款，不满足要求为**无效投标。**

**一、概述**

网络视听新媒体综合监管平台升级改造项目（以下简称“本项目”）按照北京市广播电视和网络视听行业的全流程、全要素、综合监管要求，对网络全方位管理，实现网络视听监管、网络视听舆情监管、行业网络安全监管等业务需要。一是实现网络视听内容监测、网络宣传、节目审核、精品创作、机构管理、综合业态管理等业务，为北京市网络视听行业统筹管理提供数据依据及分析建议。二是进行网络视听舆情监管，围绕北京广播电视和网络视听行业进行舆情监测及预警，实现对广电舆情的全面监测和风险预警。三是提供行业网络安全监管服务，对广电播控网络进行全面监测，掌握关键网络运行状况和安全风险，有针对性地研判预警，提升行业整体安全水平。

升级改造后的系统将扩充网络视听内容监管业务范围、提升网络视听舆情监管能力、增设行业网络安全监管能力，以及遵循集成化、一体化、数据化、网络化、智能化原则构建为各类应用提供共性服务的公共业务应用组件、数据存储分析等支撑环境，并根据等保三级要求构建相关网络安全环境。

本包实现对本市22家播出传输单位业务系统的网络安全监测，进行风险识别、威胁发现、安全事件实时告警及可视化展示等安全防护，保障播出安全、网络安全。

网络视听监管、网络视听舆情监管业务部署在北京市政务云，通过专用通信链路和软件平台相连；网络安全监测前端部署在14个区融媒体中心、北京新媒体集团等22家播出单位，行业网络安全监测业务（互联网端）软件平台部署在北京市政务云，探针等前端设备部署在各安播单位。

★本包所有具有互联网协议地址规划方式的设备软硬件均须支持 IPv6互联网协议。

★本包软件开发及部署须根据采购人要求适配相应数据库、操作系统、服务器等信创环境。

★本包软件开发需符合网络安全等级保护2.0三级防护要求。

★投标人需配合本项目第一包、第二包、第七包，做好：①智能运维、数据底座、指挥调度、数据可视化展示的数据对接及相关开发工作；②做好单点登录、用户管理的协议接口开发工作；③提供完整业务流闭环方案，做好通过北京安播PC端、北京安播移动端、短信途径向各安播单位发送告警信息、事件信息、通报信息及接收各安播单位上报信息等业务的数据对接及相关开发工作，具备信息反馈渠道，各安播单位可通过北京安播PC端、北京安播移动端完成事件查看、处置、反馈、事件消除等动作。投标人提供承诺函，格式自拟，加盖公章。

**二、采购需求一览表**

**行业网络安全监管（互联网端）软件开发需求一览表**

各部分功能需求见“三、性能配置及技术指标要求 （一）行业网络安全监管（互联网端）软件开发”

| **序号** | **名称** | | **数量** | **单位** | **备注** |
| --- | --- | --- | --- | --- | --- |
| 1 | 业务应用 | 资产管理 | 1 | 套 |  |
| 2 | 等保管理 | 1 | 套 |
| 3 | 安全监测 | 1 | 套 |
| 4 | 攻击链分析 | 1 | 套 |
| 5 | 深度融合分析 | 1 | 套 |
| 6 | 预警通报 | 1 | 套 |
| 7 | 威胁情报 | 1 | 套 |
| 8 | 全文检索 | 1 | 套 |
| 9 | 数据分析 | 网络安全数据分析管理 | 1 | 套 |
| 10 | 网络信息安全分析引擎 | 1 | 套 |
| 11 | 数据采集 | 日志数据采集 | 1 | 套 |
| 12 | 网络流量数据采集 | 1 | 套 |
| 13 | 资产发现和采集 | 1 | 套 |
| 14 | 漏洞数据采集 | 1 | 套 |
| 15 | 安全事件数据采集 | 1 | 套 |
| 16 | 数据存储 | 数据存储 | 1 | 套 |

**注：以上表中序号1至序号16，预算控制金额为：49.875万元，超出按无效处理；**

**软硬件设备需求一览表**

性能配置及技术指标要求见“三、性能配置及技术指标要求 （二）软硬件设备”。

| **序号** | **设备名称** | **数量** | **单位** | **备注** |
| --- | --- | --- | --- | --- |
| 1 | 流量探针 | 5 | 台 | 流量探针（1.7G） |
| 2 | 日志探针 | 5 | 台 | 日志探针 |
| 3 | 漏洞探针 | 5 | 台 | 漏洞探针 |
| 4 | 流量分流器 | 5 | 台 | 流量分流器 |

**注：表序号1至序号4预算控制金额为：136.5万元，超出按无效处理。**

**三、性能配置及技术指标要求**

1. **行业网络安全监管（互联网端）软件开发**

**1．业务应用**

* 1. **资产管理**
     1. **资产概况**
        1. **资产动态检测识别**

1. 具备按照单位、系统、网站、设备、软件、服务、机房、网络、数据库维度对资产数据分类及展示，具备增删改查、导入导出、批量处理等功能；
2. 具备漏洞扫描报告导入功能，类型包括主机漏洞、配置核查、WEB漏洞、弱口令等，文件格式支持xml和excel；支持对导入后的漏洞扫描报告进行管理，内容包括报告名称、报告类型、资产脆弱性数量、报告文件格式、解析模板、导入时间等；支持报告下载功能；
3. 具备对资产的脆弱性评估功能，实现资产潜在漏洞发现和管理，通过对已纳管资产数据与漏洞知识库关联匹配生成潜在漏洞信息，资产潜在漏洞信息包括资产名称、资产类型、版本型号、所属单位、首次发现时间，以资产视角展示潜在漏洞信息；
4. 具备漏洞库知识库，包括漏洞发布时间、漏洞名称、漏洞类型、危害等级、漏洞编号、CNNVD编号、CNVD编号、其他编号、漏洞来源、威胁类型等信息，支持漏洞详情查看功能。
   * + 1. **总体资产状况统计**
5. 具备对各安播单位资产统计功能，包括资产数量情况（单位数量统计、网站/系统数量统计、软件数量统计、设备数量统计和IP数量统计）、资产运营情况、资产重要程度统计、硬件资产分布情况、软件资产分布情况、系统资产分布情况、单位资产分布情况；以TOP10形式进行展示；
6. 具备资产数据展示功能，包括柱状图、环状图、矩形树图等形式。
   * 1. **资产归档**
        1. **资产归档模板管理**

具备资产归档模板管理能力，支持不同类型资产的导入模板，包括单位、设备、系统、网站、软件、机房等资产类型模板。

* + - 1. **资产数据导入、统计、展示配置**

1. 具备将填报数据按模板分类导入功能，支持展示导入结果信息，包括正常导入的资产数据、无法导入的资产数据，模板中填报数据能自动解析存入对应的数据存储结构中；
2. 具备资产导入结果统计及展示能力，对已填报单位数量及填报的数据进行统计及展示。
   * 1. **一键搜索**
        1. **资产分类规则配置**

具备资产分类规则配置功能，通过预置规则自动将原始发现的资产进入纳管状态，对资产的归属规则、运营规则和忽略规则进行配置。

* + - 1. **资产状况时间设置检索**

1. 通过关键字方式，从单位、设备、软件、服务、系统、网站、机房、网络、数据库、用户等维度，对资产进行精确检索或模糊检索，能够点击查看具体资产的详情信息；
2. 具备与、或、非等常见查询语法示例；
3. 具备通过语法规则组合对资产数据进行高级检索；
4. 具备高级筛选功能，通过关联资产、资产状态、更新时间、资产数据范围、时间范围等维度对资产进行筛选；
5. 具备历史检索记录管理功能，能够查看历史检索的资产数据范围、时间范围、检索语句等内容，历史记录不少于10条；
6. 具备将检索条件保存至“常用检索”功能，支持对“常用检索”条件的查看、选择、删除等操作。
   * 1. **资产融合**
        1. **资产自动纳管规则配置**
7. 建立资产纳管规则，包括资产归属规则、资产运营规则，自动将监测前端采集、手动录入的待纳管资产进行统一管理；支持对资产纳管规则的启用、停用等配置操作；
8. 资产归属规则：通过探针序列号、IP、域名等信息确定资产归属单位；
9. 资产运营规则：通过IP、MAC等信息自动发现资产冲突；建立置信度规则自动解决资产冲突；
10. 具备资产审核功能，对纳管规则输出的结果进行人工审核，包括新增资产、更新资产、忽略资产。
    * + 1. **资产融合规则配置**

具备资产融合规则功能，支持基于IP、所属单位、端口、协议等维度对各前端采集的原始资产数据进行自动融合，过滤重复或无效资产数据。

* 1. **等保管理**
     1. **定级备案管理**

1. 具备手动录入及模板导入等保备案信息功能，包括系统等保备案、单位等保备案两个维度。
2. 系统等保备案内容包括系统名称、系统类型、保护等级、备案单位、距离复测截止日期、备案时间、备案状态、整改情况等，支持系统备案数据的编辑、删除、导出、详情查看等操作。
3. 单位等保备案内容包括单位基本信息、已备案系统、未备案系统等，支持单位备案数据的编辑、删除、导出、详情查看等操作。
   * 1. **等保数据统计**
4. 具备行业等保工作总体情况统计功能，包括行业各级系统数量、各安播单位各级系统数量、测评情况（复测、复测逾期）、检查情况、限期整改情况和系统安全状况等；
5. 具备系统测评逾期告警功能，针对各安播单位等保系统到期未开展等保测评情况进行告警；
6. 系统测评逾期告警推送至中心平台，由中心平台对接监测中心现有短信发布模块、北京安播移动端发布平台及北京安播PC端，发布至各安播单位；
7. 具备统计结果展示功能，以柱状图、表格等形式进行展示；
8. 具备安播单位等保工作详情查看功能，包括系统数量、系统名称、备案等级、测评开展情况、整改情况、责任人与联系方式等信息。
   * 1. **检查任务管理**
9. 具备等保检查任务管理功能，支持等保检查任务的创建、编辑、删除、导出、查询等操作，指派指定人员对等保单位开展检查工作；
10. 具备等保检查任务阶段管理功能，包括创建、检查、处置、反馈、归档等阶段；
11. 具备按照安播单位、等保系统等维度对检查任务进行统计功能，内容包括等保检查项、等保检查要点、检查要点合格情况等；支持按照时间范围对检查统计结果进行筛选。
    * 1. **测评信息管理**
12. 具备备案系统测评信息管理功能，支持上传测评报告、测评合同、测评计划等文档；支持对系统测评结果信息的编辑、导入、导出、删除、查询、详情等操作；
13. 具备备案系统测评信息展示功能，包括系统名称、测评状态、测评时间、测评机构、测评师、测评分值、测评结果等内容；
14. 具备测评机构信息管理功能，支持对测评机构信息的编辑、导入、导出、删除、查询、详情等操作；
15. 具备测评机构信息展示功能，内容包括测评机构、服务范围、服务级别、有效期、地址、联系人、联系方式、传真等；
16. 具备测评师信息管理功能，支持对测评师信息的编辑、导入、导出、删除、查询、详情等操作；
17. 具备测评师信息展示功能，内容包括姓名、所在机构、从业时间、证书编号、证书级别、联系方式等。
    * 1. **等保综合分析报表**
18. 具备对各安播单位等保情况综合分析报表报告功能，报表支持以文字、表格、饼状图、柱状图等方式展示行业网络安全等级保护工作整体情况，具备报表报告预览功能；
19. 具备报表报告数据源管理功能，支持自定义数据源的来源渠道，包括本地文件、数据库的数据表等；
20. 具备报表报告数据集管理、数据目录权限设定功能，实现不同角色的访问权限控制；
21. 具备报表报告导出功能，文件格式包括Excel、Word、PDF等类型；报告周期包括年报、月报等，时间可自定义。
    1. **安全监测**
       1. **告警管理** 
          1. **威胁告警数据管理**
22. 具备告警信息展示功能，对系统发现的各类网络安全告警实时展示；
23. 具备告警处置状态记录功能，通过不同底纹颜色等方式区别告警状态处置与否；
24. 具备告警信息管理功能，支持告警信息导入、导出、批量打标签等操作，告警标签可自定义：
25. 支持对告警状态变更操作，状态包括无需处置、误报、查实需处置、已处置、IP封禁等，支持逐个操作及批量操作；
26. 具备告警统计功能，按照单位名称、时间范围、告警类型等维度对告警信息进行统计；
27. 具备告警查询功能，按照单位名称、时间范围、告警类型等维度对告警信息进行查询；
28. 具备展示历史告警查询条件记录功能，包括查询范围、时间范围、查询语句等内容，能够选择历史查询条件再次查询；
29. 支持告警信息字段配置，支持按特定字段排序；具备以柱状图、折线图等形式展示指定时间、不同类型、不同等级告警功能；
30. 支持查看告警详情，包括告警基本信息（告警类型、攻击源IP、受害者IP、告警级别等）、关联的规则信息、原始告警列表等。
    * + 1. **高级威胁创建分析联动**
31. 具备对选定的高级威胁告警信息创建研判任务；
32. 一键转入研判任务，通过攻击频次、访问关系、原始告警实现威胁分析的联动处置能力。
    * 1. **事件管理**
         1. **事件关联分析管理**
33. 具备网络安全事件生成功能，支持网络安全告警生成事件、人工添加事件等方式；事件字段包括事件标题、事件分类、事件标签列表、事件等级、上报单位、事件描述、发现时间、事发单位、事态发展概述及初判原因、响应处置要求、处置建议等内容；
34. 具备网络安全事件管理功能，包括事件审核、处置、查询、导出等操作。审核结果包括通过、不通过、无需处置；事件处置类型包括启动事件通报、启动应急、关联应急、无需处置等；事件查询支持时间范围、关键字、事件等级、事件标题、事件分类、处置状态、上报单位等维度查询；
35. 具备网络安全事件详情查看功能，包括事件基本信息、关联信息、举证信息、要素信息、处置进展、操作记录、补充信息等内容。
    * + 1. **威胁多维度综合评估分析**
36. 具备网络安全事件分类分级功能，事件分类包括恶意程序事件、网络攻击事件、数据安全事件、信息内容安全事件、违规操作事件、设备设施故障事件、安全隐患事件、异常行为事件、其他事件等内容；事件分级包括一般事件、较大事件、重大事件和特别重大事件等；
37. 具备网络安全事件全流程管理功能，包括事件待提交、待研判、被退回、待处置、处置中、已处置等；
38. 具备网络安全事件展示功能，包括列表视图、单列视图等方式。
    * 1. **数据分析**
         1. **多维数据分析**

具备多维数据分析功能，通过汇聚网络安全告警数据、网络安全事件数据，分析北京市广播电视行业安全趋势、威胁同比/环比情况，得出安播单位系统资产告警排名、情报命中情况、攻击源TOP排名等内容。

* + - 1. **图形化统计分析**

具备图形化展示功能，通过柱状图、环状图、曲线图、表格等方式对分析结果进行展示。

* + 1. **监测规则管理**
       1. **监测规则配置管理**

1. 具备告警监测规则库，内容包括有害程序、攻击利用、信息破坏、内容安全、拒绝服务、异常活动、信息收集、安全隐患、可用性、后渗透行为等威胁的识别规则；
2. 具备告警监测规则与攻击链模型各阶段映射功能；
3. 具备告警监测规则统一管理功能，包括规则新增、编辑、复制、删除、启动、导入、导出、详情、查询等。其中，规则启动包括测试启动、正式启动；规则查询包括规则名、规则来源、模板类型、数据源、规则阶段、规则状态、攻击方向、防护实体信息、规则标签、任务状态等查询条件；
4. 具备告警监测规则展示功能，支持规则字段配置。
   * + 1. **数据字段关联配置**
5. 具备对采集的网络安全原始数据关联配置功能，利用监测规则中等于、包含等条件组合，将原始数据字段与告警数据字段建立关联，实现网络安全原始数据过滤、告警自动确认、告警归并、告警基本信息字段的重新定义；
6. 具备对告警基本信息字段的自定义功能，将网络安全原始数据字段（包括源IP、目的IP、源端口、目的端口等）映射为告警基本信息字段（包括攻击源IP、受害者IP、源端口、目的端口等）。
   * 1. **资源对象管理**
7. 具备安播单位资源对象库，内容包括安播单位资产IP地址、端口、时间等资源；
8. 设计告警监测规则可直接引用安播单位资源对象库内相关资源；
9. 具备资源对象统一管理功能，包括资源对象新增、编辑、复制、删除、导入、导出、详情、查询等。
   * 1. **行业模型配置**
10. 具备广电行业规则配置功能，包括新建规则、命中规则、告警生成策略、告警归并策略等；新建规则时，支持自定义规则名称、规则版本、发布时间、规则状态、规则模板、规则描述、规则标签、规则属性等内容；
11. 通过广电行业规则组合生成网络安全告警监测模型，包括：网络攻击监测模型、应用威胁监测模型、运维管理监测模型、异常行为监测模型等；
12. 具备监测模型筛选功能，基于规则名称、数据源、任务状态、标签等多种条件对模型进行筛选。
    * 1. **数据统一检索**
         1. **数据字段关联关系配置**

具备字段关联关系配置功能，通过语法规则（and、or等）对告警基本信息字段进行组合，实现流量日志、网络日志数据精准查询。

* + - 1. **数据统一分析检索**

1. 具备统一分析检索功能，通过关键字对流量日志、网络日志数据进行模糊检索；
2. 具备检索结果展示功能，包括日志数据检索条数、日志数量时间分布、单条日志信息详情等；
3. 具备日志检索结果导出功能。
   1. **攻击链分析**
      1. **资产画像**
4. 具备资产画像功能，通过资产管理模块中的基础信息、所属安全域、关联资产、漏洞信息、变更记录等维度对安播单位资产进行画像；
5. 具备安播单位资产关联功能，关联维度包括：资产组成、拓扑结构、关键要素等，为威胁告警信息富化提供数据支撑；
6. 基于安全设备、计算设备、网络设备、终端设备等资产要素构建拓扑结构；
7. 具备资产漏洞影响范围评估功能，通过漏洞的基本信息、影响资产信息评估漏洞对业务系统的影响范围。
   * 1. **攻击者同源分析**
8. 具备攻击者同源分析功能，通过识别攻击者IP信息，归并同源IP，将属于同一攻击者的相关网络威胁进行关联、归并；
9. 具备攻击者同源分析任务管理功能，包括任务创建、概览、编辑、复制、删除等功能；
10. 具备分析任务工作台，包括数据汇聚、数据过滤、高危IP清单、攻击者画像等功能；
11. 数据汇聚：收集安全事件信息；
12. 数据过滤：通过添加可信IP或无需处置IP，过滤无效告警；
13. 高危IP清单：列表展示待处置的高危攻击者IP信息，内容包括攻击时间、告警数据来源、源IP、今日攻击次数、攻击/告警类型、告警名称、告警状态、攻击结果、受害者信息等；
14. 攻击者画像：提供攻击者IP关联告警信息补充功能，包括告警信息补录、画像信息补录等方式，形成完整的攻击者画像；
15. 具备攻击者同源分析结果展示功能，以图谱、地图、表格等方式，展示每个攻击IP的累计攻击次数、IP库标签、IP溯源信息及IP历史画像信息等内容；
    * 1. **攻击链标签建模**

具备攻击链标签建模功能，结合安播单位业务系统实际情况，设置恶意程序入侵链条、网络攻击链条的识别场景，对告警所属ATT&CK攻击链不同阶段打标签。

* + 1. **基于钻石模型分析**

1. 具备攻击总览视图，攻击链包括侦查跟踪、武器构建、载荷投递、突防利用、安装植入、通信控制、达成目标等阶段；
2. 展示每个阶段的全量告警数据；
3. 以时间轴方式展示攻击过程；
4. 支持调整告警所属的攻击链阶段；
5. 具备钻石模型分析展示功能，展示威胁相关的攻击者、受害者、基础设施和能力维度的详细信息。
   1. **深度融合分析**
      1. **失陷情报数据匹配**
6. 系统具备自动接收各监测前端日志探针、流量探针采集的安播单位业务系统网络安全数据功能；
7. 具备失陷情报数据匹配功能，通过威胁情报（威胁情报的定义详见1.9.3 威胁情报模型配置）与实际资产的比对，发现失陷资产，威胁情报包括：恶意IP地址、恶意URL、恶意DNS、恶意Email、MD5等。
   * 1. **失陷数据编码映射**
8. 具备对监测前端采集的流量数据、日志数据预处理能力，提供输入类、编码类、富化类、输出类、控制类等插件，创建数据自动处理流程，提高数据预处理工作效率；数据预处理工作包括数据质量评估、数据清理、数据集成、数据转换、数据标记等；
9. 具备数据预处理任务配置功能，任务支持引用一个或多个数据自动处理流本开展数据预处理工作；
10. 具备数据预处理任务管理功能，包括新增、运行、停止、重启、编辑、删除等；
11. 具备数据预处理任务展示功能，包括任务名称、状态、处理日志速度等；
12. 具备未解析数据当前日志、历史日志的下载、查看功能。
    * 1. **数据归一化管理**
13. 具备对各监测前端采集数据归一化管理功能，对各安播单位资产的异构日志格式进行归一化处理；
14. 对采集和处理过的安全数据进行存储，包括结构化数据、半结构化数据和非结构化数据存储；其中，对日志数据、告警信息可设置存储天数；
15. 归一化后的网络安全数据及相关日志、报告等信息全部推送至本项目数据底座治理、存储，完成相应适配工作。
    * 1. **规则关联分析**
16. 具备关联规则分析功能，通过日志、情报、资产等类型数据进行关联，发现恶意代码、异常行为等安全威胁并进行告警；
17. 具备关联分析规则管理功能，包括规则新增、编辑、分类、查询、导入、导出、删除、详情等；
18. 提供统计类、序列类、关联类规则模板库，以图形化处理的方式编排规则模型。
    * 1. **智能模型分析**

具备广电行业网络安全智能分析模型，根据各安播单位业务系统实际场景，分析采集到的网络安全数据资源，通过关联分析规则自动匹配，对发现的安全威胁进行告警，包括Web攻击、网络攻击、异常行为发现等安全威胁。

* 1. **预警通报**

将安全监测模块中监测分析产生的网站漏洞、风险和事件及手工导入的外部获取的安全事件等数据，通过日常通报、专项通报等方式，及时通报涉事的单位，督促涉事单位进行快速处置，确保问题得到及时整改、反馈、核实、归档，从而实现完整业务流程的闭环。

* + 1. **安全事件维度分析**

1. 具备安全事件日常通报发起功能，对通过研判确认的安全事件，一键发起通报；并可手动创建通报；
2. 日常监测告警生成的网络安全事件，推送至中心平台，由中心平台对接监测中心现有短信发布模块、北京安播移动端发布平台及北京安播PC端，发布至各安播单位；其中，通过北京安播移动端发布平台及北京安播PC端下发的网络安全事件信息，可携带多种类型附件；
3. 具备安全事件展示功能，通过接入事件管理模块的数据，以连线图、表格等方式展示待通报的安全事件信息和数量。
   * 1. **日常通报分析管理**
4. 具备通报事件分析功能，分析通报反馈数量、整改平均完成时间等；
5. 具备日常通报任务统计功能；能够对通报反馈情况、问题整改情况、事件处罚情况进行统计；
6. 具备日常通报任务管理功能，支持按照模板自动生成网络安全隐患告知书、事件报告；
7. 具备日常通报处置流程展示功能，流程状态包括未处置、处置中和处置完毕等；展示内容包括处置单位、处置状态、处置时间、延期状态等；
8. 具备日常通报反馈功能，支持各安播单位通过北京安播PC端上传整改报告，实现业务流程闭环处置；
9. 具备整改报告统计功能，支持按照时间、单位名称、事件类型等维度统计、检索、上传、下载整改报告；
   * 1. **专项通报分析管理**
10. 具备针对特定风险、特定事件制定专项通报任务，基于上级单位通报的网络安全风险、漏洞隐患等网络安全信息，通报各安播单位进行风险排查；
11. 专线通报任务信息推送至中心平台，由中心平台对接监测中心现有短信发布模块、北京安播移动端发布平台及北京安播PC端，发布至各安播单位；其中，通过北京安播移动端发布平台及北京安播PC端下发的专线通报任务信息，可携带多种类型附件；
12. 针对同一通报任务，具备手动添加或按组分配多个对象，并一键下发功能；
13. 具备专项通报任务配置功能，配置对象包括：通报标题、通报下发时间、通报下发单位、通报内容、风险种类、初判风险等级、初判风险类型、通报状态、处置完成时间等，并支持添加多种类型附件、多个附件功能；
14. 具备自动生成专项通报任务报告功能，报告内容包括：任务类型、任务对象、任务执行时间、任务执行结果等；
15. 具备专项通报任务报告统计功能，支持按照时间、单位名称、事件类型等维度统计、检索、上传、下载专项通报任务报告。
    * 1. **通报事件统计**

具备通报事件统计功能，按时间范围对通报事件类型、单位被通报次数、受影响资源、通报整改工作阶段、超时未反馈、被通报事件来源、被通报单位问题严重情况等维度进行统计。

* + 1. **综合通报管理**

1. 具备综合报告生成功能，支持按照时间、单位名称、系统名称、通报事件类型等维度，综合统计分析日常通报、专项通报事件，自动生成综合通报报告；
2. 提供综合报告模板管理，内容包括通报类型、通报编号、通报标题、通报基本情况（事件类型、涉事IP等、事件描述、单位名称等)、通报处理意见等；
3. 具备报告模板新建、编辑、配置、删除、检索、启用等功能；
4. 具备综合报告内容预览、编辑、导出功能，格式支持Word、PDF等。
   * 1. **通报规则配置管理**
5. 具备通报流程模板管理功能，支持对日常通报、专项通报任务的业务流程进行管理，包括创建、编辑、复制、删除等内容；
6. 具备通报流程模板编排功能，支持配置审核、重新提交、签收、执行、验证、归档等各环节，对各环节的执行时限、执行人范围、表单配置、可见范围、操作选项和消息模板进行配置；
7. 具备各类通报流程模板展示功能，以列表方式展示通报流程，包括通报类型名称、类型描述、更新时间等内容；
8. 具备通报流程模板调用功能，支持在新建日常通报、专项通报任务时选择对应的模板发起通报任务。
   1. **威胁情报**
      1. **事件深度分析引擎**
9. 具备事件深度分析引擎，利用引擎内的威胁情报库与告警管理模块产生的告警攻击源IP进行比对，实现攻击源IP详细信息富化；
10. 具备黑客属性识别功能，包括：所属组织、威胁名称、威胁类型、威胁级别、地理位置信息等；
11. 具备黑客信息识别功能，包括：攻击IP、告警类型、源MAC地址、攻击次数、载荷长度、载荷内容等；
12. 具备黑客能力识别功能，包括：攻击手段、关联资产等；
13. 具备同源攻击IP分析功能，通过引擎筛查的条件组合，实现对全量告警的同源攻击IP识别、告警；
14. 具备根据已知特征进行告警降噪功能，已知特征包括：受害IP（IP 段）、攻击源IP（IP 段）、威胁情报、威胁名称、域名、目的端口、源IP（IP段）、目的IP（IP段）等信息的降噪。
    * 1. **APT活动拓展分析**
15. 具备对APT事件分析功能，通过探针采集的攻击原始日志、原始告警对APT攻击事件所处阶段（侦察、入侵、命令控制、横向渗透、目的执行、痕迹清理）进行分析；
16. 以折线图等形式对APT攻击事件所处阶段进行展示。
    * 1. **威胁情报模型配置**
17. 具备手动、自动更新威胁情报库功能；
18. 支持第三方威胁情报导入，情报格式包括JSON格式 、STIX格式、XLSX格式、OPENIOC格式等；
19. 具备威胁情报分析模型配置功能，通过匹配IP、域名、MD5等信息，创建威胁情报分析规则。
20. 具备ATT&CK知识库，可将安全告警与ATT&CK知识库进行比对，展示告警所采用的攻击技术详情。
    1. **全文检索**
       1. **分布式数据索引**

对流量探针、日志探针采集到的全部日志创建索引，索引条件包括时间维度、日志类型等，提升系统检索速度。

* + 1. **高级汇聚数据分类查询**

具备对日志文件内容的查询功能；

1. 对不同格式（Unicode编码、UTF8编码、URL解码/编码、Hex解码/编码、Base64解码/编码、进制转换等）日志进行归一化处理、入库、统一展示；
2. 具备快捷查询功能，通过关键字查询日志内容；
3. 具备高级查询功能，通过等于、包含、不等于等语法组合，创建自定义查询条件，精确查询日志内容；
4. 具备日志查询结果详情展示功能，能够查看结果字段及对应值；
5. 具备历史查询记录管理功能，能够查看历史检索的日志查询范围、时间范围、查询语句等内容，历史记录不少于10条；
6. 具备将查询条件保存至“常用查询”功能，支持对“常用查询”条件的查看、选择、删除等操作。

**2.安全数据采集**

* 1. **日志数据采集**

1. 对接日志探针，通过SYSLOG、HTTP等协议自动接收日志探针采集到的各安播单位资产的日志信息，日志探针的采集方式包括 Syslog、SNMP Trap、文本格式、数据库、Netflow、HTTP等。
2. 具备日志探针管理功能，能够查看全部日志探针的详细信息，包括各探针接收的日志总数、解析日志总数、未解析日志总数等。
   1. **网络流量数据采集**
3. 对接流量探针，通过kafka等协议自动接收流量探针采集到的各安播单位流量信息，流量探针通过旁路镜像等方式，采集各安播单位关键系统在IPv4/IPv6双协议栈下的全部流量；
4. 具备流量探针管理功能，能够查看全部流量探针的详细信息，包括探针上传流量、平台接收流量、差值率等。
   1. **资产发现与采集**

具备安播单位资产数据自动获取、手动录入功能；

1. 对接探针，通过kafka等协议自动接收采集识别安播单位关键系统内的IP地址、MAC地址等信息，实现资产的自动获取；
2. 具备手动录入、模板导入安播单位关键系统的资产信息功能；包括资产名称、厂家、型号、IP地址、网络掩码、MAC地址等信息。
   1. **漏洞数据采集**

对接漏扫探针，通过接口对接等方式自动接收漏扫探针采集到的各安播单位关键系统的漏洞信息。

* 1. **安全事件数据采集**

按照采购人要求，对接广播电视融合媒体智慧监管平台的网站安全监测子系统，交互获取网站安全监测事件信息。

**3.安全数据处理**

1. 按照采购人统一要求进行数据标准化处理，存储入库；
2. 具备数据处理流程管理功能，以可视化拖拽等方式设计数据处理流程，包括流程创建、删除、导入、输出统计、查看、编辑、复制等功能；
3. 具备对采集到的网络安全数据进行富化处理的能力，包括字段映射、归一化数据、静态值映射、动态数据映射、字段删除、地理位置映射、字段改名、默认值填充、系统时间填充、数组拆解、RedisKV富化、日志打标、字典表等映射、字典表IP号段富化、字段加工映射等；

**4.安全数据存储**

1. 具备结构化、半结构化和非结构化数据存储功能，分类构建资产库、脆弱性库、情报库、用户库、知识库、基础库、对象库、原始库等，并集中配置管理；
2. 具备配置数据重要程度、存储天数等功能；
3. 配合第1包中标单位做好数据存储规划、实施及部署。

**5.安全数据分析**

* 1. **网络安全数据分析管理**
     1. **规则关联分析**

具备关联分析规则设计功能，通过过滤、关联统计、序列、基线日志统计、基线行为统计等基础模型，设计贴合广电业务场景的关联分析模型，包括有害程序、攻击利用、信息破坏、内容安全、拒绝服务、异常活动、信息收集、安全隐患、可用性、后渗透行为等模型；提供模型数量不少于700个。

* + 1. **攻击面安全分析（资产安全分析）**

1. 具备资产安全分析功能，将已知的特定漏洞，与漏扫探针识别出的各安播单位资产漏洞信息进行比对，筛查各安播单位业务系统是否存在该漏洞；
2. 关联预警通报模块，将筛查出的漏洞信息通知相关单位。
   * 1. **高级威胁分析**

具备高级威胁分析功能，将流量探针采集到的流量，与威胁情报模块中的威胁情报进行比对，调用样本分析引擎，筛查恶意文件，实现对恶意程序执行、恶意代码投递等伪装攻击的检测。

* + 1. **漏洞分析**

1. 具备漏洞知识库，包括公共漏洞信息、自定义漏洞信息；
2. 具备手动、自动更新漏洞知识库功能；
3. 具备漏洞分析功能，将漏洞探针采集到的漏洞信息与漏洞知识库进行匹配，识别漏洞的危害等级、类型，并进行告警；
4. 具备漏洞统计功能，按照漏洞危害等级、受影响资产数量、漏洞类型等维度统计各安播单位资产漏洞情况；
5. 具备漏洞查询功能，按照单位名称、漏洞名称、漏洞类型、漏洞危害等级等维度查询漏洞情况；
6. 具备漏洞展示功能，以表格、柱状图等方式展示各安播单位资产漏洞情况。
   * 1. **异常行为分析**
7. 构建异常行为分析模型，包括特殊端口关闭/启用模型、域名周期性解析模型、跳板机行为模型、资产异常外连模型、暴力破解模型等异常行为模型；
8. 将流量探针采集到的流量数据与异常行为模型进行比对，对发现的异常行为进行告警。
   * 1. **WebShell攻击分析**
9. 构建Webshell攻击分析模型，具备识别asp、php、jsp、cgi等网页文件构建的WEBshell攻击的能力；
10. 将流量探针采集到的流量数据与Webshell攻击分析模型进行比对，对发现的WEBshell攻击行为进行告警；
11. 具备Webshell分析内容展示功能，包括WebShell利用工具名称、攻击方向、源IP、目的IP、目的端口、目的单位、目的资产名称，通过趋势图呈现Webshell攻击的活跃度。
    * 1. **弱口令分析**
12. 构建弱口令分析模型，具备弱口令资产发现能力；
13. 将流量探针采集到的流量数据与弱口令分析模型进行比对，对发现的弱口令登录行为进行告警；
14. 具备弱口令统计功能，按照单位名称、资产名称等维度统计弱口令情况。
    * 1. **代理隧道分析**
15. 构建代理隧道分析模型，具备frp端口转发、reDuh隧道代理、reGeorg隧道代理、Tunna隧道代理等事件发现能力；
16. 将流量探针采集到的流量数据与代理隧道分析模型进行比对，对发现的代理隧道事件进行告警。
    1. **网络信息安全分析引擎**
       1. **流量检测分析引擎**

结合流量探针实现以下功能：

1. 提供流量检测分析引擎，对网络链路全流量采集、全数据分析，具备网络异常行为感知能力、多维数据索引能力、网络攻击定位与取证能力；
2. 具备告警攻击研判能力，利用双向检测机制、原始数据包和研判模型，对攻击结果进行判断，结果包括：攻击尝试、攻击成功；
3. 支持对应用层协议进行攻击检测，包括HTTP、FTP、TFTP、TLS、SSH、SMB、DNS、NFS、DHCP、SNMP等；
4. 支持对多种攻击类型进行检测，包括：漏洞利用检测、各类特征检测、恶意攻击程序检测、拒绝服务攻击检测、可疑通信检测。
   * 1. **关联分析引擎**
5. 具备关联分析引擎，根据规则关联分析（5.1.1）设计的分析模型，创建关联分析任务，生成告警、归并告警，产生安全分析结果数据，并进行告警；
6. 具备关联分析模型筛选功能，按照规则名、规则来源、模板类型、数据源、规则阶段、规则状态、攻击方向、规则标签、任务状态等条件对模型进行筛选。
   * 1. **资产分析引擎**
7. 具备资产分析引擎，利用引擎内的资产特征库与资产发现与采集模块发现的资产信息进行匹配，实现资产的精确识别；
8. 构建资产关系图谱，展示各安播单位业务系统的设备图谱。
   * 1. **样本分析引擎**

通过接收各种格式的文件，结合静态检测，动态检测和威胁情报检测技术，对恶意文件进行识别并进行告警。

1. 具备样本分析引擎，对执行文件、脚本类文件、多媒体文件、文档类文件、压缩文件等文件样本进行分析，识别恶意文件；
2. 将流量探针采集到的文件、手动上传的文件与样本分析引擎进行比对筛查，对发现的恶意文件进行告警；
3. 具备筛查结果展示功能，包括恶意文件的MD5、文件类型、文件名、检测结果、检测时间、检测状态等信息；
4. 支持恶意文件和筛查报告下载、批量下载。
   * 1. **ATT&CK分析引擎**

具备ATT&CK分析引擎，对ATT&CK知识库进行手动、自动更新；

具备视图展示功能，将系统发现的各类网络告警与ATT&CK模型各阶段进行映射，展示各阶段的告警数量。

* + 1. **情报分析引擎**

1. 具备威胁情报统计功能，统计内置威胁情报、自定义情报的数量；
2. 具备威胁情报查询功能，可对告警信息携带的恶意IP地址、恶意URL、文件MD5等信息进行查询，确认告警威胁程度；
3. 具备威胁情报展示功能，以表格形式展示威胁情报信息。
   * 1. **APT分析引擎**
4. 具备APT事件识别功能，利用探针采集的恶意文件MD5、DNS流量、TCP流量、UDP流量等信息，与事件深度分析引擎内的威胁情报库进行比对，识别APT攻击事件，并进行告警；
5. 具备APT分析引擎，联动流量探针查看原始数据包中特征告警详情，内容包括：源目IP、情报类型、攻击类型、攻击结果、告警级别等信息。
6. **软硬件设备**

**1.流量探针（1.7G）**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 硬件要求 | 标准机架式设备，冗余电源，千兆电口≥6个，千兆光口≥2个万兆光口≥2个，Console口≥1个，接口扩展板卡插槽≥2个。 |
| 2 | 性能要求 | 同时开启网络流量采集、威胁数据采集和日志上报功能情况下混合流吞吐量≥1.7Gbps，HTTP并发连接数≥300万，HTTP新建连接速率≥2万/秒；具备流量数据、威胁数据进行采集、还原、解密、外发等能力，支持不少于19种协议还原能力。 |
| 3 | 部署方式 | 支持通过流量镜像的方式获取核心交换机网络流量，实现网络流量数据采集、威胁检测和日志外发，支持通过重置会话的方式阻断TCP威胁会话连接，支持通过流量被动识别资产。 |
| 4 | 离线采集 | 具备离线采集功能，通过手动Pcap导入方式对离线流量进行采集，支持批量导入，支持流量回放。 |
| 5 | 协议解析 | 具有自定义解析流量能力，支持基于正则表达式、固定长度等提取模式对应用流量解析。支持基于全部会话流的攻击检测功能，无漏报。 |
| 6 | 协议采集 | 支持采集和分析的协议包括：HTTP、FTP、TFTP、SMTP、TLS、SSH、IMAP、SMB、DNS、NFS、DHCP、SNMP、SIP、RDP等。  具备加密流量协议解析能力，能够分析镜像加密流量，确保发现安播单位系统终端、服务器、虚拟机等违规外联、数据外发泄露等行为，无漏报。 |
| 7 | 协议还原 | 具备还原多种文件传输协议能力，包括：Web（HTTP）、FTP、SMB等。 |
| 8 | 威胁检测 | 检测常见的溢出攻击、跨站脚本、SLQ注入、拒绝服务、跨站请求伪造、目录遍历、webshell上传等。 |
| 9 | 具备攻击检测能力的扩展功能，支持自定义恶意文件、自定义漏洞、自定义间谍软件、自定义威胁情报等。 |
| 10 | 具备间谍软件检测能力，检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、隧道、代理通道、后门程序、远控木马等。 |
| 11 | 支持对检测的告警事件结合检测机制、原始数据包和研判模型等规则进行深层次研判，给出告警事件的攻击结果。 |
| 12 | 告警过滤 | 具备攻击告警的过滤能力，能够针对IP地址或端口对攻击告警进行过滤，支持攻击特征高亮展示。 |
| 13 | 本地情报 | 本地集成威胁情报库，支持基于威胁情报的失陷主机和挖矿主机检测，情报数量≥100万条。 |
| 14 | 加密协议解析 | 具备基于SSL协议的SMTPS、POP3S、IMAPS、HTTPS流量解密功能。 |

**2.日志探针**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 硬件要求 | 标准机架式设备，内存容量≥16GB，硬盘容量≥4TB，千兆电口≥6个，千兆光口≥4个，扩展插槽≥2个。 |
| 2 | 性能要求 | 日志采集处理能力≥2500EPS，最大日志源≥150个，本次不少于35个日志源授权。 |
| 3 | 采集方式 | 具备Syslog、SNMP Trap、JDBC、FTP、SFTP等协议的日志采集能力，采集网络设备、安全设备、主机及业务系统等资产日志；具备通过规则对各类日志归一化、过滤、合并、富化的能力。 |
| 4 | 资产信息 | 具备对所采集资产的信息管理功能，包括名称、类型、厂商、序列号、IP/MAC、地理位置、联系人等信息。 |
| 5 | 日志展示 | 具备对所采集资产的运行时长、日志源数量、关联事件数、告警总数、已保存日志时长、存储空间等情况展示功能。 |
| 6 | 事件搜索 | 具备自定义“事件查询条件”功能，支持多条件组合查询并保存为策略功能，支持对不同场景的自定义策略查询。 |
| 7 | 归一化 | 具备日志归一化功能，实现对多元异构日志格式进行统一描述和处理。 |
| 8 | 资产管理 | 支持自定义资产类型及资产属性；支持对资产打标签，支持对标签内容进行查询和管理。 |
| 9 | 解析字段 | 日志解析内置不少于60个字段，属性字段可扩展，可根据审计需要自行创建字段，内置及新增的所有字段均可参与事件查询、关联分析和报表数据源统计。 |
| 10 | 关联分析 | 支持展示日志属性之间的聚合关系，支持手动选择日志属性，支持属性调整，具备显示多维事件分析图功能。 |
| 11 | 安全分析场景 | 支持多种安全分析场景，包括恶意代码、可疑控制、入侵利用、违规行为、嗅探行为、关联审计等。 |

**3.漏洞探针**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 硬件要求 | 标准机架式设备，10/100/1000M Base-TX≥6个，千兆光口≥4个，扩展槽≥2个，USB接口≥2个，具备显示面板；内存容量≥32G，硬盘容量≥1TB。 |
| 2 | 性能要求 | 并发任务数≥10个，单任务支持扫描IP数≥150个，支持IP地址数量≥1024个，网页扫描并发任务数≥7个域名（具备网页并发扫描能力），具备系统漏洞检测、web漏洞检测、数据库漏洞检测、配置合规检测、弱口令检测等检测功能。 |
| 3 | 扫描任务 | 具备系统扫描、Web扫描、弱口令扫描分析功能，支持对指定IP地址段多种扫描任务一键下发功能。 |
| 4 | 扫描策略 | 支持立即扫描、定时扫描、周期性扫描、断点续扫等扫描任务执行方式。 |
| 5 | 分析报告 | 根据系统漏洞、Web漏洞、弱口令扫描结果自动生成分析报告。 |
| 6 | 扫描模式 | 具备标准扫描、快速扫描、完全扫描、深度扫描等扫描模式。 |
| 7 | 漏洞特征库 | 覆盖CNVD、CNNVD等多种漏洞标准。特征库漏洞数不少于40万个，支持手动更新、在线更新。 |
| 8 | 统计视图 | 具备不同维度的统计视图，包括系统情况、WEB应用情况、风险分布等。 |
| 9 | 检测类型 | 支持扫描通用操作系统、交换路由设备、安全设备、物联网设备、虚拟化、中间件、国产操作系统、国产数据库、国产办公软件、WEB网站、虚拟化软件及大数据组件。 |
| 10 | 资产管理 | 支持资产信息管理，含资产名称、IP、MAC、负责人等。 |

**4.流量分流器**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 指标要求 |
| 1 | 设备要求 | 配置48个10/100/1000BASE-T以太网端口，4个万兆SFP+接口  交换容量≥2.4Tbps/24Tbps，包转发率≥552Mpps/762Mpps 交流电源模块×2，风扇插×2个 MAC地址条目≥320K |
| 2 | 功能要求 | 支持 MAC 认证、802.1x 认证、Portal 认证 |
| 3 | 支持IGMP v1/v2/v3； |
| 4 | 支持SNMP v1/v2/v3、Telnet； |
| 5 | 支持VxLAN二层、三层网关，支持三层路由功能 |
| 6 | ★支持IPV6； |
| 7 | 配齐光模块 |

**四、售后服务要求**

投标人应提供详细的项目《需求理解分析》《软件设计开发方案》《项目实施方案》《质保期内服务方案》《质保期内应急预案》。

**（一）需求理解分析**

投标人应提供详细的《需求理解分析》，要求内容全面、详细具体、理解准确、重难点分析到位，紧贴我市广播电视网络视听安全监测态势感知，并能提出切实可行的解决办法。

**（二）软件设计开发方案**

投标人应按照采购需求，制定详细的软件开发设计方案，包括软件功能需求分析、系统总体架构设计、代码编写、测试和上线部署调试、系统联调、软件测评、验收等内容及计划安排，提供设计说明书、设计图等材料。

配合本项目的第三方软件测评机构做好中心平台软件测评、安全测评并按要求进行相应整改。

**（三）项目实施方案**

投标人应提供详细的《项目实施方案》。内容包括：组织架构、进度计划、软件开发、安装实施、突发事件处置等内容。

投标人应遵守北京市及采购人有关规定，主动配合监管平台项目其他建设单位、软件测评、安全测评单位、密码应用评估单位、监理单位的工作。

按照采购人要求，对接广播电视融合媒体智慧监管平台的网站安全监测子系统，构建统一的网络安全态势感知平台。

合同签订后，60个自然日内，完成购置软硬件设备交货；合同签订后，180个自然日内，完成软件研发、部署、调试等工作。

投标人应参与本项目数据标准化方案制定工作，提供网络安全监测业务专业意见。

投标人应配合第一包做好数据可视化相关工作。

★项目实施过程中，采购人根据业务工作实际情况，可对本项目业务功能需求进行深化设计，中标人应配合采购人进行设计方案、软件开发的调整，功能达到采购人要求。投标人提供承诺函，格式自拟，加盖公章。

中标人负责协调各安播单位安装探针等前端设备。

**（四）项目实施团队**

投标人应为本项目实施配备专门的项目技术团队，包括项目负责人、软件研发人员、产品安装调试人员等，负责本项目中心平台软件开发、产品安装调试和布线等具体实施工作。

项目实施团队中，软件研发人员不少于10名，进行网络安全监管软件开发研发设计；产品安装调试人员不少于5名，进行软硬件设备安装调试。项目负责人具有5年以上相关项目经验，具备软件开发、网络规划、系统调试能力，具备信息系统项目管理师（高级）资格证书；软件研发人员需具备3年以上软件开发工作经验，具备CISP-CISD（注册信息安全开发人员）或CISP-DSG（注册数据安全治理专业人员）证书；产品安装调试人员需具备3年以上网络规划、设备安装、系统调试工作经验，具备CISAW（安全集成）或CISAW（安全运维）证书；团队人员需提供人员简历等材料。

软件研发人员、设备安装调试人员的交通、食宿等费用由投标人承担，且技应遵守采购人现场的各项规章制度和安全操作规程，并服从采购人管理。

**（五）培训**

投标人免费提供设备原理、操作使用、维护等培训，项目验收前提供1次培训，质保期内每年1 次。

**（六）质保期内服务**

投标人应提供本项目质量保证期内的详细服务方案、应急预案。应设有热线服务电话，当出现突发事故事件时，采购人在任何时候可以得到及时响应和事故事件及时处置。

**1. 运行维护**

投标人应提供《质保期内服务方案》，内容包括：组织架构、职责分工、业务运营、系统维护等，内容应详细具体、可行且具有针对性，确保业务顺畅开展，确保系统稳定运行。

质保期内应当按照采购人的要求，每月至少进行1次巡检维护，安全播出重要保障期、重要安全检查前进行专项巡检，满足广播电视安全播出工作要求。

（1）运行维护内容

运行维护内容应当包括但不限于：

检查维护软硬件设备运行状态、日志；备份数据、日志；检查维护病毒库、规则库等软件运行和版本升级更新情况，保持当前版本最新；资产梳理、安全策略优化、故障排除等，保障监管平台网络安全、稳定运行。

（2）运行维护报告

运行维护报告包括：内容概述、设备软硬件主要指标及运行状态、日志情况、故障现象及处理、软件更新情况、规则库更新、策略调优、维护日期以及维护人员签字等内容。

每次维护工作完成，应向采购人提交维护报告。

**2.维护团队**

本项目质量保证期内，投标人应提供网络安全专业维护团队，专门负责监管平台网络安全运维保障工作，应明确维护团队成员职责任务。质量保证期内维护团队成员相对稳定，人员数量不少于4人，应具备CISP或CISAW证书及2年以上网络安全项目运维工作经验。

维护人员应遵守采购人各项规章制度、安全操作规程等相关规定，并服从采购人管理，配合采购人做好网络安全保障有关工作。

**3. 应急处置**

投标人应提供《质保期内应急预案》，内容包括：组织架构、职责分工、设备抢修、应急处置等，详细具体可行且具有针对性的，确保网络安全突发事件事故得到及时有效处置，保障平台安全稳定运行。

投标人应提供7×24小时专人电话支持服务，出现网络安全事件事故时，30分钟内响应，4小时内到达故障现场，备用设备板卡或部件在8个小时内送达现场。故障处理完成后，应急处置人员应向采购人提交应急处置情况报告。

应急处置人员到达现场后，即使不是合同中的设备出现故障（含软件系统故障），投标人有责任帮助或协同采购人查找问题所在，并帮助采购人解决问题。

**★4. 现场技术支持（**投标人提供承诺函，格式自拟，加盖公章**）**

（1）广播电视安全播出重要保障期（元旦、春节、两会、十一等），按照采购人要求，投标人安排1名技术人员现场值守服务，处置突发故障，保障平台安全稳定运行。

（2）质量保证期内，投标人应安排1名网络安全专业技术人员提供5×8小时驻场技术服务。人员要求具有CISP或CISAW等网络安全资质证书，主要工作为协助做好网络安全运营，分析网络安全告警，处置网络安全事故事件，维护软硬件设备确保其正常运行，编写相关技术材料等。

（3）技术人员提供现场技术支持服务的交通、食宿等费用由中标人承担，且技术人员应遵守采购人现场的各项规章制度和安全操作规程，并服从采购人管理。

**5. 备品备件**

投标人应备有充足的备品备件，能为采购人提供7×24小时优质、迅速、及时的备品备件技术支持，不能由于备品备件等不足而影响监管平台安全稳定运行。

投标人提供详细的备品备件清单。

**五、交货**

交货时间：购置软硬件设备，合同签订后60个自然日内；

研发软件，合同签订后180个自然日内。

交货地点：北京市广播电视监测中心指定地点。

**六、试运行**

软件研发部署、设备安装、系统调试等工作完成后，且整体项目达到初验标准后，本包进行初验，投入试运行；试运行期不少于180个自然日，试运行期出现的问题全部解决后，申请项目验收。

**七、验收**

本项目验收条件为：

1.研发软件、购置软硬件设备全部到货并符合采购要求；

2.按要求完成设备安装、策略部署、调试等工作；

3.设备试运行期满并且出现的问题全部解决；

4.项目文档资料齐全并符合要求；

5.配合测评机构完成本项目的软件测评、网络安全等级保护三级的测评、密码应用评估，并对测评和评估不合格项完成整改。

上述5个条件全部满足后，北京市广播电视监测中心组织专家依据项目合同和国家行业标准及相关规定，对项目进行验收。

**八、质量保证**

投标人应承诺提供的货物是全新的、未使用过的，并符合招标文件要求及投标文件技术描述中规定的质量、规格和性能要求。

★本项目所有货物质量保证期为：自项目通过终验之日起2年。

**九、知识产权**

投标人必须为本项目提供满足需要的所有软、硬件使用授权许可，如若发生侵犯知识产权、专利权、所有权、版权或软件正版化等行为时，其侵权责任与采购人无关，由投标人承担相应的责任，并不得损害采购人的利益。

本项目所开发软件的著作权在内的全部知识产权归采购人所有，软件开发完成后，中标人须将软件开发的所有成果，包括设计文档、用户文档、数据库设计文档、软件源代码、软件运行程序、安装使用手册等全部交付采购人。

**十、廉政要求**

投标人和采购人承诺共同加强廉洁自律、反对商业贿赂。

1. 投标人不向采购人工作人员行贿或馈赠礼金、有价证券、贵重礼品；
2. 投标人不报销应由采购人或工作人员支付的费用；
3. 投标人不向采购人工作人员支付劳务报酬；不安排采购人工作人员参加宴请及娱乐活动。

**十一、采购标的所属行业**

本项目采购标的属于《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）中的：**工业**。

# 第六章 合同草案条款

**网络视听新媒体综合监管平台升级改造项目**

**（第XX包：XXXXX）采购合同**

北京市广播电视监测中心

2024年 月 日

**网络视听新媒体综合监管平台升级改造项目**

**（第XX包：XXXXX）采购合同**

甲方：北京市广播电视监测中心

地址：北京市通州区达济街5号院

法定代表人：石东正

项目联系人：孙强

联系方式：55565332

乙方：

地址：

法定代表人：

项目联系人：

联系方式：

**一、合同书**

根据《中华人民共和国民法典》等国家相关法律法规，甲方同意乙方作为网络视听新媒体综合监管平台升级改造项目（第XX包：XXXXX）的服务商。甲乙双方经协商一致订立本合同，甲乙双方应严格遵照执行。甲方网络视听新媒体综合监管平台升级改造项目中第XX包：XXXXX经华采招标集团有限公司以\_\_\_\_\_\_\_\_\_号招标文件在国内公开招标。经评标委员会评定，\_\_\_\_\_\_\_\_\_\_\_\_\_(乙方)为中标人。甲、乙双方同意按照下面的条款和条件，签署本合同。

**第一条 合同文件组成**

下列文件均为本合同不可分割的组成部分，互为补充和解释，如有不清或相互矛盾之处，以所列顺序在前的为准，但甲乙双方有特别约定的除外：

1.本合同条款

2.中标通知书

3.招标文件及其澄清文件

4.投标文件及其澄清文件

5.形成合同的其他有关文件，包括甲乙双方就具体服务内容签订的补充合同。

**第二条 合同术语定义**

除非另有特别的解释或说明，在本合同中及与合同相关的，甲乙双方另行签署的其他文件（包括但不限于本合同的附件）中，下述词语均按照如下定义进行解释：

1.“甲方”系指 北京市广播电视监测中心。

2.“乙方”系指根据合同规定向甲方提供服务的具有法人资格的实体；即中标人。

3.“合同”系指甲乙双方签署的，合同格式中载明的甲乙双方所达成的约定，包括构成合同的所有附件、附录和构成合同的所有文件。

4.“服务”系指乙方根据合同规定须向甲方提供的全部服务。

**第三条 服务内容及地点**

1.本合同的服务范围是指乙方按照网络视听新媒体综合监管平台升级改造项目（第XX包：XXXXX）招标文件要求为甲方提供相应服务：

2.实施地点：甲方指定地点。

3.交货时间：合同签订后60个自然日内，乙方将合同货物送到甲方指定地点。

4.交货地点：甲方指定地点。

5.交货方式：现场核对交货。乙方负责办理运输和保险，将货物运抵现场。有关运输和保险等的一切费用由乙方承担。

6.安装调试：设备交货后180个自然日内完成设备安装、调试、布线调试等工作。

**第四条 服务权限**

1.乙方作为甲方选定的服务商，必须根据甲方要求，承担在网络视听新媒体综合监管平台升级改造项目（第XX包：XXXXX）投标文件中向甲方承诺的服务范围内的相关工作。

2.任何情况下，未经甲方书面同意，乙方不得向第三方转让甲方在本合同中授予乙方的权限，不得超越甲方授权范围。否则甲方有权取消乙方的中标人资格。

**第五条 特别承诺**

乙方应保证无任何第三方就乙方向甲方提供的服务主张任何权利。如果任何第三方就乙方向甲方提供的服务主张任何权利，乙方须与第三方交涉并承担由此而产生的一切法律责任和费用，并赔偿因此给甲方造成的一切损失，以及甲方为反驳第三方的主张、向乙方主张权利所支付的各项费用，包括但不限于调查费、律师费、诉讼费等。

**第六条 合同金额及付款方式**

1.本合同总价为 元人民币,大写： 。

2.货物和数量

本合同货物及数量（详见分项价格一览表）。

**分项价格一览表**

单位：人民币:元

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **分项名称** | **制造商/生产厂家** | **产地** | **品牌、规格、型号** | **单价（元）** | **数量** | **单位** | **合计（元）** | **分项总计（元）** |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| **总价（元）** | | | **大写人民币：** | | | | | ¥ | |

3.本合同的付款方式为：

合同款支付方式结合项目成交金额和财政资金批复情况另行约定。合同款支付需以相应财政资金实际拨付至甲方账户为前提，若因相应财政资金未能及时到账而导致的延期支付，不应视为甲方违约，付款时间相应顺延。

4.乙方应向甲方提供符合国家相关税务规定的等额正式发票，乙方未按本合同约定向甲方提供发票的，甲方有权拒绝支付合同款，并不视为甲方违约。乙方对发票的合规性负责，如因乙方所开具的发票不合规给甲方造成的任何损失，全部由乙方承担。

甲方开票信息为：

户名：北京市广播电视监测中心

税号：1211000079755080XU

5.乙方户名、开户银行名称和账号为：

户名:

开户行:

帐号:

6.甲方支付的合同款已经包含了乙方为完成项目所需的全部费用，除合同另有明文规定外，甲方不再承担该项目其他任何费用，亦不再向乙方支付其他任何费用。

7.与该项目相关的所有费用支出，均需符合相关要求，乙方需配合甲方相关检查、延伸审计，提供相关合同、凭据、票据、支出凭证、签收单等材料。

**第七条 双方的责任、权利及义务**

（一）甲方的责任、权利及义务

1.甲方向乙方提出服务工作的内容、完成时间、完成质量等具体要求，并审定乙方提交的委托项目工作方案和配套工作计划。

2.甲方对乙方的工作可提出改进和纠正意见。

3.甲方检查监督乙方完成委托项目工作的进度，对于乙方不履行合同、不适当履行合同等行为，甲方有权要求乙方立即更正，并采取其他补救措施

4.组织专家或者通过评估，对乙方提交的委托项目工作成果的质量进行评审和验收。

5.甲方根据乙方开展工作的实际情况支付给乙方所需费用。

6.甲方应向乙方提供为完成服务所必需的资料和工作条件。

7.甲方接受乙方提交的符合本合同约定条件的工作成果或者相关文件。

8.负责按照合同约定收集、整理与委托事项有关的项目背景资料及相关技术资料和数据并提供给乙方。

9.负责委托项目所涉及的、与甲方有关的外部联系和协调工作。

（二）乙方的责任、权利和义务

1.乙方保证具有签订与履行本合同的能力和具备相应资质，保证承办的工作人员具有履行本合同义务的相应能力和资质，保证提供的服务合法且不侵犯任何第三方合法权益。

2.乙方按照甲方要求，完成甲方指定服务内容。

3.乙方认真按照合同要求完成委托项目工作，随时接受甲方的检查监督，并为检查监督提供便利条件。

4.有权接受甲方按照合同约定支付的委托报酬。

5.乙方发现甲方提供的技术资料、数据有明显错误和缺陷的，有权于收到上述资料后3日内书面通知甲方进行补充、修改。如逾期未提出异议的，则视为甲方提交的资料、数据符合合同约定的条件。

6.乙方在其经营许可的范围内，依本合同的约定向甲方提供专业的服务，并在规定的委托项目工作时间期限内完成委托项目的工作。

7.乙方应当遵守国家法律、法规和行业行为准则为甲方完成委托项目的工作；乙方提交的工作成果必须达到合同约定的要求，并对其完成的委托项目工作成果全面负责。

8.甲方对乙方提交的委托项目工作成果提出质疑或者要求乙方答复时，乙方须在收到甲方的质疑后2个工作日内给予书面解释或者答复。

9.除双方另有约定外，为本项目进行调查研究、分析论证、试验测定以及到外地进行调研、收集资料所发生的费用，由乙方自行承担；乙方自行负担因履行本合同产生的各项税负。

10.乙方在履行合同期间使用的由甲方提供或者支付费用的设备设施，属于甲方的财产，乙方在完成委托项目并向甲方提交工作成果时，应当将设备设施归还给甲方。

11.未经甲方书面同意，乙方不得将承办项目全部或者部分承办任务转委托其他第三方机构或组织承担。

**第八条 合同执行**

1.甲乙双方签订、变更、中止或者终止政府采购合同的相关条款应遵守《中华人民共和国政府采购法》第五章政府采购合同的规定。

2.本合同其效力、解释、履行和争议的解决，适用于中华人民共和国法律，属中华人民共和国法律管辖。

**第九条 项目验收**

1.到货验收：货物运抵甲方指定场所后，甲方、乙方、监理方对货物数量、规格等进行核对验收。如发现货物名称、数量、规格配置等与合同不符，甲方有权要求乙方立即更换或者提出索赔要求。

2.初验：项目各包整体完成开发、安装调试、组网、联调联测后，甲方组织初验，初验通过后出具初验报告。

3.终验：初验通过后，开始试运行，试运行期不得少于180天。项目整体试运行期满、相关问题全部排除、通过测评，且项目文档资料齐全并符合要求，可以申请项目验收，甲方组织终验，终验通过后出具终验报告。

4.如乙方提交的工作成果未通过甲方验收的，乙方应当在甲方规定的期限内进行修改并承担修改费用，并重新申请进行验收；如乙方未在甲方规定的期限内完成修改工作或者经修改后仍未能通过验收的，乙方应当承担违约责任并赔偿由此给甲方造成的全部损失。

**第十条 质保期限**

1.本包质量保证期2年，质量保证期从网络视听新媒体综合监管平台升级改造项目整体通过终验之日起计算。

2.乙方在质量保证期内负责维修、更换所有产品本身原因造成损坏的部件，并承担由此发生的费用（甲方人为因素造成的故障、毁损除外）。更换后的部件应满足本合同的规格要求。

**第十一条 税费**

1.根据国家现行税法规定，应当对甲方征收的与本合同有关的一切税费均由甲方负担。

2.根据国家现行税法规定，应当对乙方征收的与本合同有关的一切税费均由乙方负担。

3.在中国境外发生的与本合同执行有关的一切税费均由乙方负担。

**第十二条 保密条款**

双方承诺，对因履行本合同所知悉对方尚未进入公知领域的信息承担保密义务，未经双方书面同意不得向本合同以外任何其他方泄露，或用于本合同以外的任何其他目的（详见附件：保密协议）。

**第十三条 知识产权**

1.双方合作期间产生的知识产权归甲方单独所有，乙方不得擅自使用或转让给第三方。

2.乙方提供的相关产品应是自行开发的或具备合法、合规授权，满足知识产权方面的有关规定和要求。

3.乙方保证向甲方提供的服务成果是其独立实施完成，不存在任何侵犯第三方专利权、商标权、著作权等合法权益。如因乙方提供的服务成果侵犯任何第三方的合法权益，导致该第三方追究甲方责任的，乙方应负责解决并赔偿因此给甲方造成的全部损失。

4.双方确定，甲方有权利用乙方按照本合同约定提供的研究开发成果，进行后续改进。由此产生的具有实质性或创造性技术进步特征的新的技术成果及其权利归属，由甲方享有。

5本项目所开发软件的著作权在内的全部知识产权归采购人所有，软件开发完成后，中标人须将软件开发的所有成果，包括设计文档、用户文档、数据库设计文档、软件源代码、软件运行程序、安装使用手册等全部交付采购人。

**第十四条 廉政承诺条款**

1.合同双方承诺共同加强廉洁自律、反对商业贿赂。

2.甲方及其工作人员严格遵守《北京市政商交往负面清单》和《北京市广播电视监测中心政商交往正负面清单》等相关廉洁纪律规定。

3.甲方及其工作人员不得收受可能影响正常执行公务的礼品、礼金、消费卡和有价证券、股权、其他金融产品等财物，不得收受其他明显超出正常礼尚往来的财物；不得在乙方报销应由本单位或个人支付的费用；不得以参与项目实施为名，接受乙方从该项目中支取的劳务报酬；不得参加乙方安排的可能影响公正执行公务的宴请或者旅游、健身、娱乐等活动。

4.乙方不得向甲方及其工作人员馈赠可能影响公正执行公务的礼品、礼金、消费卡和有价证券、股权、其他金融产品等财物，不得馈赠其他明显超出正常礼尚往来的财物；不得为其报销应由甲方单位或个人支付的费用；不得向甲方工作人员支付劳务报酬；不得安排甲方工作人员参加可能影响公正执行公务的宴请或者旅游、健身、娱乐等活动。

5.乙方的股东、董事、监事、高层管理人员、合作项目负责人及工作人员为甲方员工的亲友或与甲方有密切关系的，应在合作前，以书面方式全面、如实告知。

**第十五条 违约责任**

1.如果乙方未能在合同规定的期限或甲方书面同意延长的期限内提供服务，乙方需按日向甲方支付违约金，违约金的计算标准为按日支付合同价款的万分之五。如果乙方延期达 日，甲方可以解除或部分解除本合同，同时乙方承担合同总额 %的违约金。违约金不足以弥补甲方损失的，乙方应补足违约金不足部分。

2.如乙方提供服务不能满足合同约定及甲方要求，甲方有权解除本合同，并要求乙方返还甲方已支付的费用，并承担合同总金额 %的违约金。违约金不足以弥补甲方损失的，乙方应当补足。

3.因为乙方违约行为甲方行使解除权的，自甲方向乙方发出解除或部分解除本合同的书面通知到达乙方时，本合同即告解除或部分解除。甲方依据法律法规和本合同的相关规定解除或部分解除本合同后，有权选择其他有能力的服务商重新作为合同乙方，另行签订服务合同，提供同类或类似服务。

**第十六条 合同解除**

1.如果乙方破产、解散、清算、停业、濒临破产或因其他原因无力履行本合同时，甲方可在任何时候以书面通知乙方解除本合同。自甲方向乙方发出解除本合同的书面通知到达乙方时，本合同即告解除。

2.本合同解除后，根据合同履行情况，甲方可以要求乙方恢复原状、采取补救措施，并有权要求赔偿损失。

**第十七条 不可抗力**

1.本合同所称不可抗力是指不能预见、不能避免并不能克服的客观情况，包括但不限于战争、严重火灾、水灾、台风和地震、政策法规的变更以及其他双方书面同意属于不可抗力的情形。

2.受不可抗力影响的一方应在不可抗力发生后，以最快的方式在最短的时间内通知另一方，并在不可抗力发生后10日内，将有关部门出具的证明文件直接送达或邮寄另一方。

3.当不可抗力事件发生时，执行合同的期限可相应延长，不视为任何一方违约。如果延长期限后合同仍不能履行的，双方可协商终止本合同。若合同终止，双方互不承担违约责任。但因一方迟延履行导致不可抗力的，不能免除责任。

**第十八条 争议的解决**

1.本合同依中华人民共和国现行法律法规（不包括香港和澳门特别行政区及台湾地区的法律法规）签署并据其解释。

2.在执行本合同过程中，双方如若发生争议，应先协商解决，协商达成一致意见，须以书面形式并加盖公章确认方可有效；协商不成时，任何一方均有权将争议提交至甲方所在地有管辖权的人民法院通过诉讼方式解决。

**第十九条 附则**

1.本合同经双方法定代表人或授权代表签字加盖公章后生效。签字日期不一致的，以最后签字日期为本合同生效日期。双方在加盖有效印章时务必加盖骑缝章。

2.本合同一式陆份，以中文书写，甲方执肆份，乙方执贰份，具有同等法律效力。

3.如需修改或补充本合同内容，经协商，双方应签署书面修改或补充协议，并将其作为本合同的组成部分。

4.下述合同附件为本合同不可分割的部分并与本合同具有同等效力：

（1）供货范围及分项价格表

（2）技术规格

（3）交货时间及交货批次

（4）服务承诺

（以下为签字盖章页*）*

甲方（盖章）：北京市广播电视监测中心 乙方（盖章）：

法定代表人或授权代表： 法定代表人或授权代表：

（签字） （签字）

签署日期： 签署日期：

地址：北京市通州区达济街5号院 地址：

邮政编码：101117 　 邮政编码：

电话：殷悦 　 电话：

联系人：55565330 联系人：

开户银行：北京银行潞城支行 开户银行：

账号：20000003326820112001009 　 账号：

**二、中标通知书**

**三、招标文件**

**（主要内容）**

**四、投标文件**

**（主要内容）**

**第七章 投标文件格式**

**投标人编制文件须知**

1、投标人按照本部分的顺序编制投标文件（资格证明文件）、投标文件（商务技术文件），编制中涉及格式资料的，应按照本部分提供的内容和格式（所有表格的格式可扩展）填写提交。

2、对于招标文件中标记了“实质性格式”文件的，投标人不得改变格式中给定的文字所表达的含义，不得删减格式中的实质性内容，不得自行添加与格式中给定的文字内容相矛盾的内容，不得对应当填写的空格不填写或不实质性响应，否则**投标无效**。未标记“实质性格式”的文件和招标文件未提供格式的内容，可由投标人自行编写。

3、全部声明和问题的回答及所附材料必须是真实的、准确的和完整的。

# 一、资格证明文件格式

**投标文件（资格证明文件）封面（非实质性格式）**

**投 标 文 件**

**（资格证明文件）**

**项目名称:**

**项目代理编号：**

**投标人名称：**

1 满足《中华人民共和国政府采购法》第二十二条规定及法律法规的其他规定

1-1营业执照等证明文件

### 1-2 投标人资格声明书（实质性格式）

**投标人资格声明书**

致：采购人或采购代理机构

在参与本次项目投标中，我单位承诺：

1. 具有良好的商业信誉和健全的财务会计制度；
2. 具有履行合同所必需的设备和专业技术能力；
3. 有依法缴纳税收和社会保障资金的良好记录；
4. 参加政府采购活动前三年内，在经营活动中没有重大违法记录（重大违法记录指因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚，不包括因违法经营被禁止在一定期限内参加政府采购活动，但期限已经届满的情形）；
5. 我单位不属于政府采购法律、行政法规规定的公益一类事业单位、或使用事业编制且由财政拨款保障的群团组织（仅适用于政府购买服务项目）；
6. 我单位不存在为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后，再参加该采购项目的其他采购活动的情形（单一来源采购项目除外）；
7. 与我单位存在“单位负责人为同一人或者存在直接控股、管理关系”的其他法人单位信息如下（如有，不论其是否参加同一合同项下的政府采购活动均须填写）：

|  |  |  |
| --- | --- | --- |
| 序号 | 单位名称 | 相互关系 |
| 1 |  |  |
| 2 |  |  |
| … |  |  |

上述声明真实有效，否则我方负全部责任。

投标人名称（加盖公章）： \_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

说明：供应商承诺不实的，依据《政府采购法》第七十七条“提供虚假材料谋取中标、成交的”有关规定予以处理。

2 落实政府采购政策需满足的资格要求（如有）

2-1中小企业声明函

说明：

（1）如本项目（包）不专门面向中小企业预留采购份额，资格证明文件部分无需提供《中小企业声明函》。

（2）如本项目（包）专门面向中小/小微企业采购，须提供《中小企业声明函》（实质性格式）。

（3）如本项目（包）预留部分采购项目预算专门面向中小企业采购，要求供应商以联合体形式参加采购活动，且联合体中中小企业承担的部分达到一定比例的，须提供《联合协议》；要求获得采购合同的供应商将采购项目中的一定比例分包给一家或者多家中小企业的，须提供《拟分包情况说明及分包意向协议（类型一）》。

（4）其他

1）中小企业参加政府采购活动，应当出具此格式文件。《中小企业声明函》由参加政府采购活动的投标人出具。联合体投标的，《中小企业声明函》由牵头人出具。

2）对于联合体中由中小企业承担的部分，或者分包给中小企业的部分，必须全部由中小企业制造、承建或者承接。供应商应当在声明函“项目名称”部分标明联合体中中小企业承担的具体内容或者中小企业的具体分包内容。

3）对于多标的的采购项目，投标人应充分、准确地了解所投产品制造企业信息。对相关情况了解不清楚的，不建议填报本声明函。

（5）温馨提示：为方便广大中小企业识别企业规模类型，工业和信息化部组织开发了中小企业规模类型自测小程序，在国务院客户端和工业和信息化部网站上均有链接，投标人填写所属的行业和指标数据可自动生成企业规模类型测试结果。

### 中小企业声明函（货物）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库﹝2020﹞46号）的规定，本公司（联合体）参加*（单位名称）*的*（项目名称）*采购活动，提供的货物全部由符合政策要求的中小企业制造。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. （*标的名称*），属于（*采购文件中明确的所属行业*）；制造商为（企业名称），从业人员人，营业收入为万元，资产总额为万元1，属于（中型企业、小型企业、微型企业）；

2. （*标的名称*），属于（*采购文件中明确的所属行业*）；制造商为（企业名称），从业人员人，营业收入为万元，资产总额为万元，属于（中型企业、小型企业、微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

1从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

**中小企业声明函（服务）格式**

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库﹝2020﹞46 号）的规定，本公司 （联合体）参加（*单位名称*）的（*项目名称*）采购活动，服务全部由符合政策要求的中小企业承接。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. （*标的名称*） ，属于（*采购文件中明确的所属行业*）；承建（承接）企业为（*企业名称*），从业人员 人，营业收入为 万元，资产总额为 万元[[1]](#footnote-1)，属于（*中型企业、小型企业、微型企业*）；

2. （*标的名称*） ，属于（*采购文件中明确的所属行业*）；承建（承接）企业为（*企业名称*），从业人员 人，营业收入为 万元，资产总额为 万元，属于（*中型企业、小型企业、微型企业*）；

......

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

|  |
| --- |
| 1从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。 |

**残疾人福利性单位声明函格式**

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**（请进行勾选）**：

**□不属于符合条件的残疾人福利性单位。**

**□属于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：

2-2 其它落实政府采购政策的资格要求（如有）

3 本项目的特定资格要求（如有）

3-1联合协议（如有）（实质性格式）

**联合协议（若本项目适用）**

\_\_\_\_\_\_ 、 \_\_\_\_\_ 及 \_\_\_\_\_就“\_\_\_\_\_\_\_\_（项目名称）”\_\_\_\_包招标项目的投标事宜，经各方充分协商一致，达成如下协议：

1. 由\_\_\_\_\_\_\_\_\_牵头，\_\_\_\_\_\_\_\_\_、\_\_\_\_\_\_\_\_\_\_参加，组成联合体共同进行招标项目的投标工作。
2. \_\_\_\_\_\_为本次投标的牵头人，联合体以牵头人的名义参加投标，联合体中标后，联合体各方共同与采购人签订合同，就采购合同约定的事项对采购人承担连带责任。
3. 联合体各方均同意由牵头人代表其他联合体成员单位按招标文件要求出具《授权委托书》。
4. 牵头人为项目的总负责单位；组织各参加方进行项目实施工作。
5. \_\_\_\_\_\_负责\_\_\_\_\_，具体工作范围、内容以投标文件及合同为准。
6. \_\_\_\_\_\_负责\_\_\_\_\_，具体工作范围、内容以投标文件及合同为准。
7. \_\_\_\_\_\_负责\_\_\_\_\_（如有），具体工作范围、内容以投标文件及合同为准。
8. 本项目联合协议合同总额为\_\_\_\_\_\_\_\_元，联合体各成员按照如下比例分摊（按联合体成员分别列明）：

（1）\_\_\_\_\_\_为□大型企业□中型企业、□小微企业（包含监狱企业、残疾人福利性单位）、□其他，合同金额为\_\_\_\_\_元；

（2）\_\_\_\_\_\_为□大型企业□中型企业、□小微企业（包含监狱企业、残疾人福利性单位）、□其他，合同金额为\_\_\_\_\_元；

（…）\_\_\_\_\_\_为□大型企业□中型企业、□小微企业（包含监狱企业、残疾人福利性单位）、□其他，合同金额为\_\_\_\_\_元。

1. 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。
2. 其他约定（如有）：\_\_\_\_\_\_\_。

本协议自各方盖章后生效，采购合同履行完毕后自动失效。如未中标，本协议自动终止。

联合体牵头人名称：\_\_\_\_\_\_ 联合体成员名称：\_\_\_\_\_\_

盖章：\_\_\_\_\_\_ 盖章：\_\_\_\_\_\_

联合体成员名称：\_\_\_\_\_\_

盖章：\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

注：联合体各方成员应在本协议上共同盖章，不得分别签署协议书。

3-2其他特定资格要求

4 投标保证金凭证/交款单据扫描件或复印件（如有）

# 二、商务技术文件格式

**投标文件（商务技术文件）封面（非实质性格式）**

**投 标 文 件**

**（商务技术文件）**

**项目名称:**

**项目代理编号：**

**投标人名称：**

1 投标书（实质性格式）

**投标书**

致：（采购人或采购代理机构）

我方参加你方就\_\_\_\_\_\_\_\_\_\_\_（项目名称，项目代理编号）组织的招标活动，并对此项目进行投标。

1. 我方已详细审查全部招标文件，自愿参与投标并承诺如下：

（1）本投标有效期为自提交投标文件的截止之日起\_\_\_\_\_个日历日。

（2）除合同条款及采购需求偏离表列出的偏离外，我方响应招标文件的全部要求。

（3）我方已提供的全部文件资料是真实、准确的，并对此承担一切法律后果。

（4）如我方中标，我方将在法律规定的期限内与你方签订合同，按照招标文件要求提交履约保证金，并在合同约定的期限内完成合同规定的全部义务。

2. 其他补充条款（如有）：\_\_\_\_\_\_\_\_\_\_\_。

与本投标有关的一切正式往来信函请寄：

地址\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 传真\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

电话\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 电子函件\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

投标人名称（加盖公章） \_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

2 授权委托书（实质性格式）

**授权委托书**

本人\_\_\_\_\_\_\_（姓名）系\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（投标人名称）的法定代表人（单位负责人），现委托\_\_\_\_\_\_\_（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清确认、递交、撤回、修改\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（项目名称）响应文件和处理有关事宜，其法律后果由我方承担。

委托期限：自本授权委托书签署之日起至响应有效期届满之日止。

代理人无转委托权。

投标人名称（加盖公章）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

法定代表人（单位负责人）（签字或盖章）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

委托代理人（签字/签章）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

法定代表人（单位负责人）有效期内的身份证**正反面**扫描件或复印件：

|  |  |
| --- | --- |
|  |  |

委托代理人有效期内的身份证**正反面**扫描件或复印件：

|  |  |
| --- | --- |
|  |  |

说明：

1.若供应商为事业单位或其他组织或分支机构（仅当招标文件注明允许分支机构投标的），则法定代表人（单位负责人）处的签署人可为单位负责人。

2.若投标文件中签字之处均为法定代表人（单位负责人）本人签署，则可不提供本《授权委托书》，但须提供《法定代表人（单位负责人）身份证明》（实质性格式）。

3.供应商为自然人的情形，可不提供本《授权委托书》。

**附：法定代表人（单位负责人）身份证明**

致：（采购人或采购代理机构）

兹证明，

姓名：\_\_\_\_性别：\_\_\_\_年龄：\_\_\_\_职务：\_\_\_\_

系 （投标人名称）的法定代表人（单位负责人）。

附：法定代表人（单位负责人）有效期内的身份证正反面扫描件或复印件。

|  |  |
| --- | --- |
|  |  |

投标人名称（加盖公章）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

法定代表人（单位负责人）（签字或盖章）：\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

3 开标一览表（实质性格式）

**开标一览表**

项目代理编号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 项目名称：\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **投标人名称** | **投标报价** | |
| **大写** | **小写** |
|  |  |  |  |

注：1.此表中，每包的投标报价应和《投标分项报价表》中的总价相一致。

2.本表必须按包分别填写。

投标人名称（加盖公章）：\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

4 投标分项报价表（实质性格式）

**投标分项报价表**

项目代理编号：\_\_\_\_\_\_\_\_ 项目名称：\_\_\_\_\_\_\_\_\_\_ 报价单位：人民币元

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 分项名称 | 制造商 | 产地/国别 | 制造商统一信用代码 | 制造商规模 | 品牌 | 规格、型号 | 单价（元） | 数量 | 合价（元） |
| 1 |  |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |  |
| ... |  |  |  |  |  |  |  |  |  |  |
| 总价（元） | | | | | | | | | |  |

**说明：制造商规模请填写：“中型”、“小型”、“微型”或“其他”。**

注：1.本表应按包分别填写。

2.如果不提供分项报价将视为没有实质性响应招标文件。

3.上述各项的详细规格（如有），可另页描述。

投标人名称（加盖公章）：\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_\_月\_\_\_\_\_\_日

5 合同条款偏离表（实质性格式）

**合同条款偏离表**

项目代理编号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 项目名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **对本项目合同条款的偏离情况（**应进行选择，未选择**投标无效）：**  **□无偏离**（如无偏离，仅选择无偏离即可；无偏离即为对合同条款中的所有要求，均视  作供应商已对之理解和响应。）  **□有偏离**（如有偏离，则应在本表中对偏离项逐一列明，否则**投标无效**；对合同条款中  的所有要求，除本表列明的偏离外，均视作供应商已对之理解和响应。） | | | | | |
| 序号 | 竞争性招标文件条目号（页码） | 竞争性招标文件要求 | 响应文件内容 | 偏离情况  （据实填写） | 说明 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注： “偏离情况”列应据实填写“正偏离”、“负偏离”。

投标人名称（加盖公章）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_年\_\_\_\_月\_\_\_\_日

6 采购需求偏离表（实质性格式）

**采购需求偏离表**

项目代理编号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 项目名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 招标文件条目号(页码) | 招标文件要求 | 响应内容 | 偏离情况  （据实填写） | 说明 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：

1. 对招标文件中的所有商务、技术要求，除本表所列明的所有偏离外，均视作供应商已对之理解和响应。此表中若无任何文字说明，内容为空白的**响应无效**。

2.“偏离情况”列应据实填写“正偏离”、“负偏离”或“无偏离”。

供应商名称（加盖公章）：\_\_\_\_\_\_

日期：\_\_\_\_年\_\_\_\_月\_\_\_\_日

7 中小企业声明函

说明：

1）中小企业参加政府采购活动，应当出具此格式文件。《中小企业声明函》由参加政府采购活动的投标人出具。联合体投标的，《中小企业声明函》由牵头人出具。

2）对于联合体中由中小企业承担的部分，或者分包给中小企业的部分，必须全部由中小企业制造、承建或者承接。供应商应当在声明函“项目名称”部分标明联合体中中小企业承担的具体内容或者中小企业的具体分包内容。

3）对于多标的的采购项目，投标人应充分、准确地了解所投产品制造企业信息。对相关情况了解不清楚的，不建议填报本声明函。

4）温馨提示：为方便广大中小企业识别企业规模类型，工业和信息化部组织开发了中小企业规模类型自测小程序，在国务院客户端和工业和信息化部网站上均有链接，投标人填写所属的行业和指标数据可自动生成企业规模类型测试结果。

**中小企业声明函（货物）格式**

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库﹝2020﹞46号）的规定，本公司（联合体）参加（*单位名称*）的（*项目名称*）采购活动，提供的货物全部由符合政策要求的中小企业制造。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. （*标的名称*），属于（*采购文件中明确的所属行业*）；制造商为（*企业名称*），从业人员 人，营业收入为 万元，资产总额为 万元，属于（*中型企业、小型企业、微型企业*）；

2. （*标的名称*），属于（*采购文件中明确的所属行业*）；制造商为（*企业名称*），从业人员 人，营业收入为 万元，资产总额为 万元，属于（*中型企业、小型企业、微型企业*）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：\_\_\_\_\_\_\_\_

日 期：\_\_\_\_\_\_\_\_

|  |
| --- |
| 1从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。 |

**残疾人福利性单位声明函格式**

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**（请进行勾选）**：

**□不属于符合条件的残疾人福利性单位。**

**□属于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：

8 招标文件要求提供或投标人认为应附的其他材料

1. [↑](#footnote-ref-1)