电子化政府采购

招标文件

采购编号:NBZFCG2023C026G

项目名称:宁波市政务信息化网络数据安全一体化指挥系统建设项目

宁波市政府采购中心

二 〇 二 三 年

**目 录**

**第一章 专用部分**

第一部分 投标邀请

第二部分 项目需求说明及评标标准

第三部分 投标人须知资料表

**第二章 通用部分**

第四部分 投标人须知

第五部分 合同格式

第六部分 投标文件格式

第七部分 其他文件格式

第一部分 **投标邀请**

日期：2023年11月3日

宁波市政府采购中心就以下项目进行公开招标，现邀请合格投标人进行加密电子投标。

一、项目基本情况

1、项目编号：NBZFCG2023C026G

2、项目名称：宁波市政务信息化网络数据安全一体化指挥系统建设项目

3、采购预算（最高限价）：人民币1696.8万元

4、采购需求：宁波市政务信息化网络数据安全一体化指挥系统建设，详见项目需求说明。

5、合同履行期限：合同签订起至2025年1月项目竣工止。

6、联合体投标：不接受

二、投标人的资格要求

1、符合《政府采购法》第二十二条的规定且未列入“www.creditchina.gov.cn、www.ccgp.gov.cn”网站失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信记录名单在禁止参加采购期限的供应商。

2、特定资格要求：无。

3、落实政府采购政策需满足的资格要求：**要求合同分包，提供分包意向承诺。接受分包合同的中小企业与分包企业之间不得存在直接控股、管理关系。**

**（1）投标人为大型企业的，分包意向协议中中小企业合同金额应不低于合同总金额的10%;**

**（2）投标人为中小企业的，视同符合资格条件，不得将合同分包给大中型企业。**

三、获取招标文件：

1、获取时间：至 2023年12月26日9：30。

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

3、采购文件免费获取。

四、电子投标和开标事项

1、政采云电子投标开标平台：www.zcygov.cn

2、提交电子投标文件截止时间：2023年12月26日9：30。

3、电子投标文件解密开标时间：投标截止时间后半小时内。

4、开标现场地址：宁波市鄞州区宁穿路1901号市政务服务中心四楼开标区（具体场所安排详见电子指示屏幕）。

5、如认为需要，投标人可以选择递交备份投标文件，采用数据电文形式，以U盘形式存储，同时附带纸质说明（明确供应商全称、项目名称及编号、联系人及联系手机码号），并在投标截止时间前，通过邮寄方式，送达指定地点，逾期送达或未密封将被拒收。

6、备份文件收件人：周老师/朱老师/洪老师0574-87187932、87187168、87187962；收件地址：宁波市宁穿路1901号市政务服务中心5楼501室、506室。（收件时间：上午9:00-11:30，下午13:30-17:00，节假日、双休日除外，推荐使用中国邮政速递和顺丰快递。）

五、公告期限：自公告之日起5个工作日。

六、其他补充事项

1、供应商认为采购文件使自己的权益受到损害的，可以自获取采购文件之日或者采购文件公告期限届满之日（公告期限届满后获取采购文件的，以公告期限届满之日为准）起7个工作日内，对采购文件需求的以书面形式向采购人提出质疑，对其他内容的以书面形式向采购人和采购代理机构提出质疑。质疑供应商对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉。质疑函范本、投诉书范本请到浙江政府采购网下载专区下载。

2、本项目在四楼开标区视频直播评审现场。

七、对本次采购提出询问，请按以下方式联系

1、采购人：宁波市大数据发展管理局

联系人：杨信磊 联系电话：0574-89182601

地址：宁穿路2001号市行政中心一号楼

2、集中采购机构：宁波市政府采购中心

项目联系人：陈先生 联系电话：0574-87187959 传真：0574-87187961

地址：宁波市鄞州区宁穿路1901号市政务服务中心五楼

**第二部分 项目需求说明及评标标准**

**特别申明：**

1. **任何违反《政府采购法实施条例》第20条规定的要求均为无效采购需求。**
2. **不得将注册资金、资产总额、营业收入、从业人员、利润、纳税额等供应商规模条件作为资格要求或者评审因素。**
3. **招标文件要求提供的合同、资质、证明等信息按要求编制到投标书中。**
4. **采购需求中出现的品牌型号仅供参考，欢迎其他相当的产品投标。**
5. **投标人在政采云平台解密出来的投标报价与投标文件中投标报价不一致的，以投标文件中的投标报价为准。**
6. **本项目标的对应所属行业：软件和信息技术服务业、工业。**

选择视频述标的，请在投标截止时间前，通过邮寄方式，送达指定地点，逾期送达或未密封将被拒收。邮寄地址及收件人同备份文件接受相关信息。选择现场述标的，请根据四楼大屏显示信息，在项目对应开标室等候。

**项目需求说明**

**标包1：宁波市政务信息化网络数据安全一体化指挥系统建设**

**一、项目建设目标**

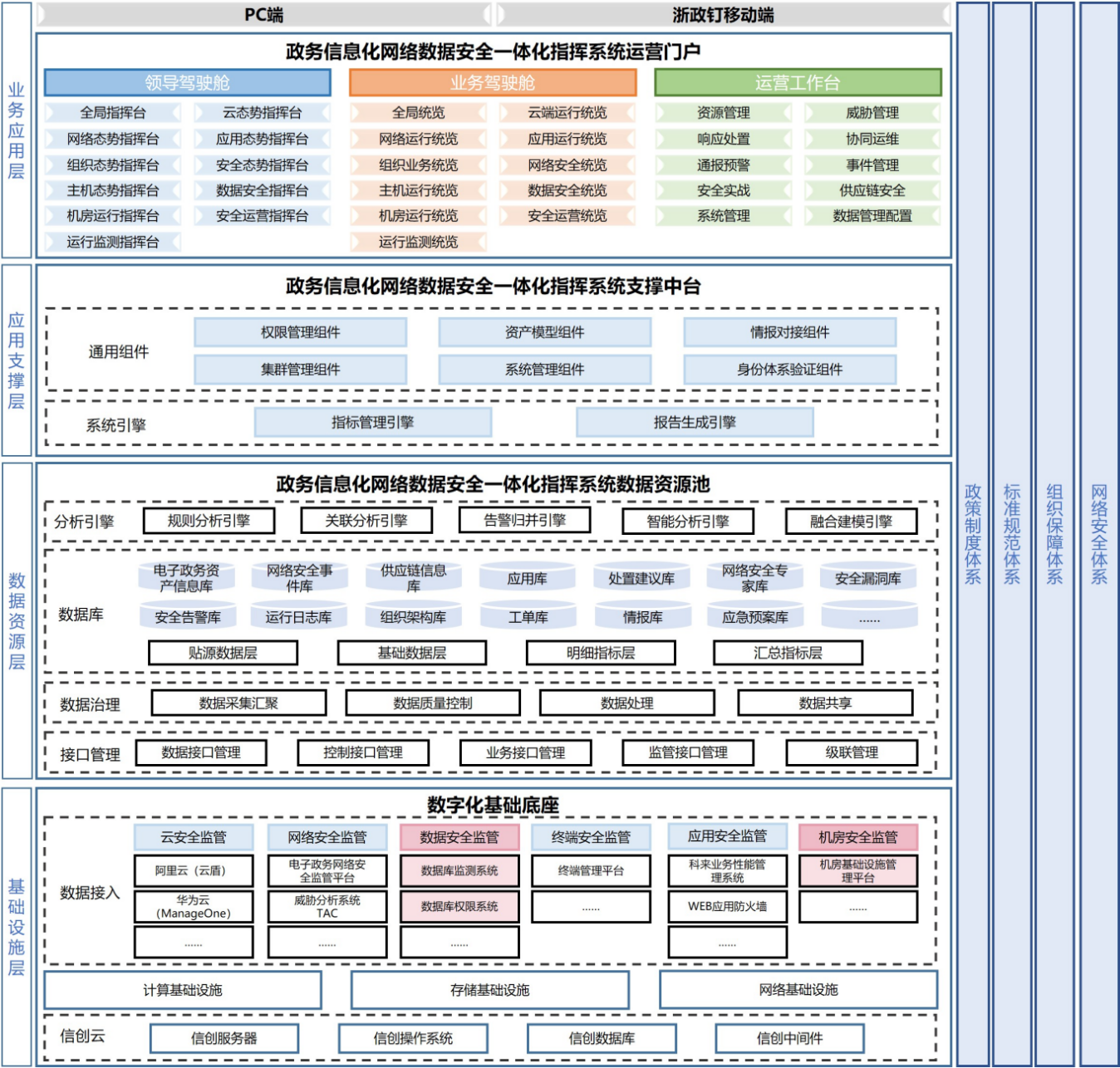
根据省市网络安全要求，从“构建覆盖云、网、数、端、应用全链路安全监测体系，提升一体化网络安全监测预警能力”出发，按照“四横四纵”的架构，建设“资产清、态势明、反应灵、可视化、成体系”的宁波市政务信息化网络数据安全一体化指挥系统，充分依托宁波市现有和补充建设的安全监管能力，形成包含“监测预警能力中心、安全防护能力中心、响应处置能力中心、协同运维能力中心、联动指挥能力中心”五大能力中心的一体化网络安全防护体系，为宁波市数字化改革工作夯实基础。

**二、项目建设规模**

项目采用市级投资建设模式，统一部署，区（县、市）级共同使用。项目建设覆盖宁波市本级和10个区（县、市）和2个功能园区，用户范围涉及宁波市市县两级的电子政务行业网络安全监管部门、市县两级业务部门、运营工作团队及人员等。

**三、项目建设内容**

宁波市政务信息化网络数据安全一体化指挥系统建设项目总体架构如下图所示：



**注：数字化基础底座红色区块为本项目建设内容，其他为利用已有系统的能力。**

宁波市政务信息化网络数据安全一体化指挥系统建设内容包括政务信息化网络数据安全一体化指挥系统运营门户、支撑中台、数据资源池和数字化基础底座。运营门户建设内容包括基于PC端和浙政钉移动端的领导驾驶舱、业务驾驶舱、运营工作台。系统支撑中台建设内容包括通用组件和系统引擎。数据资源池是通过数据采集和数据治理后形成的，为一体化指挥系统的支撑中台和运营门户提供数据支撑服务，建设内容包括分析引擎、数据库、数据治理和接口管理四部分。数字化基础底座建设是利用宁波市政务云资源部署在政务外网运行，按照信创环境部署需求，配置信创服务器、信创操作系统、信创数据库和信创中间件等。接入各个维度的安全监管平台、安全设备的监管数据，形成系统数字化基础底座。

项目建设过程中需符合上级文件要求完成相关系统的对接工作。

**四、项目采购清单**

| **序号** | **建设内容** | **数量** |
| --- | --- | --- |
| **（一）业务应用层建设** | | |
| 1.1 | 领导驾驶舱 | |
| 1.1.1 | 全局指挥台 | 1 |
| 1.1.2 | 云态势指挥台 | 1 |
| 1.1.3 | 网络态势指挥台 | 1 |
| 1.1.4 | 应用态势指挥台 | 1 |
| 1.1.5 | 组织态势指挥台 | 1 |
| 1.1.6 | 安全态势指挥台 | 1 |
| 1.1.7 | 主机态势指挥台 | 1 |
| 1.1.8 | 数据安全指挥台 | 1 |
| 1.1.9 | 机房安全指挥台 | 1 |
| 1.1.10 | 安全运营指挥台 | 1 |
| 1.1.11 | 运行监测指挥台 | 1 |
| 1.1.12 | 区县级驾驶舱 | 1 |
| 1.2 | 业务驾驶舱 | |
| 1.2.1 | 全局统览 | 1 |
| 1.2.2 | 云端运行统览 | 1 |
| 1.2.3 | 网络运行统览 | 1 |
| 1.2.4 | 应用运行统览 | 1 |
| 1.2.5 | 组织业务统览 | 1 |
| 1.2.6 | 网络安全统览 | 1 |
| 1.2.7 | 主机运行统览 | 1 |
| 1.2.8 | 数据安全统览 | 1 |
| 1.2.9 | 机房运行统览 | 1 |
| 1.2.10 | 安全运营统览 | 1 |
| 1.2.11 | 运行监测统览 | 1 |
| 1.3 | 运营工作台 | |
| 1.3.1 | 资源管理 | 1 |
| 1.3.2 | 威胁管理 | 1 |
| 1.3.3 | 响应处置 | 1 |
| 1.3.4 | 协同运维 | 1 |
| 1.3.5 | 通报预警 | 1 |
| 1.3.6 | 事件管理 | 1 |
| 1.3.7 | 安全实战 | 1 |
| 1.3.8 | 供应链安全 | 1 |
| 1.3.9 | 系统管理 | 1 |
| 1.3.10 | 数据管理配置 | 1 |
| **（二）应用支撑层建设** | | |
| 2.1 | 通用组件 | |
| 2.1.1 | 资产模型组件 | 1 |
| 2.1.2 | 权限管理组件 | 1 |
| 2.1.3 | 集群管理组件 | 1 |
| 2.1.4 | 系统管理组件 | 1 |
| 2.1.5 | 情报对接组件 | 1 |
| 2.1.6 | 身份体系验证组件 | 1 |
| 2.2 | 系统引擎 | |
| 2.2.1 | 指标管理引擎 | 1 |
| 2.2.2 | 报告生成引擎 | 1 |
| **（三）数据资源层建设** | | |
| 3.1 | 分析引擎 | |
| 3.1.1 | 规则分析引擎 | 1 |
| 3.1.2 | 关联分析引擎 | 1 |
| 3.1.3 | 告警归并引擎 | 1 |
| 3.1.4 | 智能分析引擎 | 1 |
| 3.1.5 | 融合建模引擎 | 1 |
| 3.2 | 数据库 | |
| 3.2.1 | 数据分层 | 1 |
| 3.2.2 | 数据建模 | 1 |
| 3.2.3 | 专题库 | 1 |
| 3.3 | 数据治理 | |
| 3.3.1 | 数据采集汇聚 | 1 |
| 3.3.2 | 数据质量控制 | 1 |
| 3.3.3 | 数据处理 | 1 |
| 3.3.4 | 数据共享 | 1 |
| 3.4 | 接口管理 | |
| 3.4.1 | 数据接口管理 | 1 |
| 3.4.2 | 控制接口管理 | 1 |
| 3.4.3 | 业务接口管理 | 1 |
| 3.4.4 | 监管接口管理 | 1 |
| 3.4.5 | 级联管理 | 1 |
| 3.4.6 | 其他系统数据接入 | 1 |
| 3.4.7 | 接口清单 | 1 |
| 3.5 | 第三方威胁情报对接（**采购人现有天融信、安恒第三方威胁情报服务，供应商投标响应第三方威胁情报服务如与现有品牌重复的，将作无效投标处理**） | 2 |
| **（四）基础设施层建设** | | |
| 4.1 | 数据安全监管建设 | |
| 4.1.1 | 数据库监控系统 | 1 |
| 4.1.2 | 数据库权限系统 | 1 |
| 4.2 | 机房安全监管建设（机房基础设施管理平台） **注：其中投标时需提供终端和显示器节能产品认证证书，未提供将作无效投标处理** | 1 |
| 4.3 | 安全防护软件和设备建设 | |
| 4.3.1 | 防火墙 | 4 |
| 4.3.2 | web应用安全检测系统 | 1 |
| **（五）国产信创软件采购** | | |
| 5.1 | 操作系统 | 28 |
| 5.2 | 应用中间件 | 11 |
| 5.3 | 数据库管理软件 | 7 |

**（采购清单中除硬件设备外，本项目软件部分属于定制化开发，潜在投标商可根据自身情况自行选择合适的技术路线和产品，制定配套实施方案。）**

**五、设计及建设要求**

**（一）建设原则**

1、五维覆盖，一体推进

把握“云、网、数、端、应用”五维一体化思想，突出体系化，统筹设计指挥系统架构，既加强顶层设计又坚持重点突出，既抓好当前要求又谋划长远发展，既适应业务需求又保障能力支撑。突出一体化，横向联动各市级部门，纵向贯通省网络安全监测平台、区（县、市）网络安全监测设施和系统。

2、问题导向，服务实战

以问题为导向，聚焦网络安全突出问题和薄弱环节，构建“资产链路要清晰、资源利用要高效、安全防护要统一、协同处置要提升、工作步调要一致”的一体化指挥体系。以服务实战为出发点，加强战略谋划和战术设计，提档升级各项措施，构建从制度、管理和技术有机衔接的网络安全综合防御体系，增强战略定力。

3、安全可控，闭环管理

切实加强网络安全风险管控，加强“事前、事中、事后”全生命周期管理。以事件高效、规范处置为导向，建立事件发现、事件预警、事件处置、事件反馈、事件复核的闭环流程，形成网络化、多层次、大纵深的立体式闭环管理体系。

4、能力可靠，防护提升

以需求为前提，建设宁波市政务信息化网络数据安全防护能力。立足云安全、网络安全、数据安全、终端安全、应用安全、物理安全等安全防护需求，集成现有的网络安全能力和补充建设相关安全能力，发挥网络安全能力的支撑和服务功能，切实提升宁波市政务信息化网络数据安全防护能力，让建设成果惠及宁波市所有政务网络。

**（二）业务目标**

实现资产底数清的业务目标：通过系统对接、主动探测、被动识别、用户报送等手段汇聚电子政务资产信息，建立电子政务资产信息库，并根据电子政务资产变化情况及时更新，实现动态掌握宁波市政务信息化资产情况的目标。

实现指挥一体化的业务目标：通过系统接入已有的以及补充建设的监管能力，全面掌握宁波市云、网、数、端、应用、机房等电子政务资产运行状况和安全态势，实现一体化指挥的目标，提升用户分析、决策和指挥能力。

实现事件处置联动的业务目标：通过初步建立省市县三级贯通，市级部门横向联动的机制，提升运营工作人员效率，实现事件处置协同合作、上下贯通联动，事件处置闭环、高效、规范的目标。

实现高效协同运维的业务：通过剧本编排、一键封堵/封停等能力建设，实现网络安全防护自动化能力、响应处置效率提升的目标；通过协同运维能力建设，实现高效协同安全运维的目标。

实现安全能力提升和数据级联对接的业务目标：通过政务信息化网络数据安全监管能力建设，提升电子政务资产监管能力、事件监测和隐患监测能力、组织保障能力。构建宁波市政务网络安全数据资源池满足与省大数据局数据对接的要求，按照国家《政务外网安全监测平台基本数据定义和级联接口技术要求V2.0》文件要求与全省一体化网络安全平台对接相关数据（告警数据、安全事件、资产信息、漏洞信息、威胁情报、文件报表等）。

**（三）建立宁波市政务信息化网络安全数据资源池**

要求在项目设计和实施过程中通过内生和外联等方式采集、存储政务信息化网络数据安全相关数据，建立覆盖云、网、数、端、应用、机房等多个维度的数据信息，为威胁监测、预警提供数源。

**（四）提升宁波市政务信息化网络安全监测预警能力**

基于系统建设形成的网络安全数据资源池，通过对数据的分析和学习建立各种分析模型，并不断优化提高事件分析的准确，分析模型包括智能失陷主机分析、信息智能探测、暴力破解智能分析、账号明文传输检测、后门木马检测、主机挖矿检测、病毒扩散分析、僵尸网络检测、数据泄漏检测、账号共享检测、外联CC检测和会话风险检测等，通过多维度特征过滤实现特征值筛选，使用各类探测训练评分模型，对不同的行为进行评分，最终输出事件分析结果。

**六、项目进度要求**

中标方按照项目总体建设进度要求，分阶段制定合理的工作进度计划，并且根据招标方要求进行调整和细化，给出具体安排及工期。

项目实施时间从双方签订合同起，中标方须在规定时间内完成招标方规定和要求的建设内容，于2025年1月完成项目终验。

**七、具体建设要求**

本项目主要包括业务应用层建设、应用支撑层建设、数据资源层建设、基础设施层建设及系统安全建设等内容。

* 1. **业务应用层建设**

业务应用层是系统的展现层和实战应用平台，适用于PC端平台和浙政钉移动端，包括领导驾驶舱、业务驾驶舱和运营工作台。

* 1. **领导驾驶舱**

领导驾驶舱，面向宁波市市县两级电子政务行业网络安全监管部门用户，显示所辖范围政务云态势信息，重在统计分析综合结果。领导驾驶舱包括宁波市市级电子政务行业网络安全监管部门领导驾驶舱和10个区（县、市）以及2个功能园区的领导驾驶舱，PC端建设内容包括全局指挥台、云态势指挥台、网络态势指挥台、应用态势指挥台、组织态势指挥台、安全态势指挥台、主机态势指挥台、数据安全指挥台、机房运行指挥台、安全运营指挥台和运行监测指挥台等11个应用场景，并为各区（县、市）开发区县级驾驶舱。

浙政钉移动端的领导驾驶舱同样具备市级、区（县、市）及功能园区的展示视角，具体实现主要依靠角色所具有的权限。

* + 1. **全局指挥台**

全局指挥台支持在PC端和浙政钉移动端上展示，为领导提供了解当前电子政务外网运行状态的全局视角，主要包含云态势、主机态势、网络态势、应用态势、组织态势、安全态势、机房运行、数据安全、运行监测、安全运营等10个子指挥台的主要信息统览。

* + 1. **云态势指挥台**

云态势指挥台支持在PC端和浙政钉移动端上展示当前政务云整体运行状态信息，包含云资产数据、云流量数据、云告警数据、云工单数据等。

从范围角度，覆盖全市云资源的安全与运维概况，提供政务云运行数据，辅助市级领导做整体决策；从业务系统资产角度，从业务出发，通过业务系统维度分析全市业务系统涉及的云上服务器、网络、应用资源运行情况。使用场景：向市级及区（县、市）级领导和相关人员，展示全市或本区县内的业务系统云端运行与安全概况。

* + 1. **网络态势指挥台**

网络态势指挥台展示当前政务外网环境下的流量信息，包含全局流量态势、局部流量态势、网络丢包监测、网络延时监测、网络协议分析、应用分布分析、网络攻击趋势等。

浙政钉移动端直观展示全局流量态势趋势图、网络攻击趋势图、网络丢包率、网络协议和应用分布图。

* + 1. **应用态势指挥台**

应用态势指挥台展示当前政务云环境下的全局应用信息，偏应用层面的健康度运行统计，以及不少于17项重点应用的安全运行现状，目标是监控与辅助指挥。包括应用态势整体概览、重点应用系统运行告警展示、重点应用系统网络安全事件展示等。

浙政钉移动端展示重点应用活跃用户数、资源使用负载情况以及展示告警信息等。

* + 1. **组织态势指挥台**

领导驾驶舱的组织态势指挥台支持PC端和浙政钉移动端展示，将所属云、网、端、应用相关的信息。包括综合管理视角展示政务云、网络和主机的运行安全数据，按组织管理视角展示政务云、网络、主机的运行、安全告警、安全工单等信息。通过地图的方式，全面综合政务云、网络和主机的运行安全数据，通过橙、红、绿三种颜色帮助用户判断区域事态的紧迫性。

* + 1. **安全态势指挥台**

安全态势指挥台展示当前网络安全态势信息，包含安全综合态势、脆弱性威胁态势、资产安全态势、横向威胁态势（应用与应用、主机与主机、部门与部门之间的威胁态势）、外部威胁态势、外联威胁态势和安全告警态势等。

浙政钉移动端展示当前网络的整体安全态势、重点网络安全事件以及网络安全事件处置信息等。

* + 1. **主机态势指挥台**

主机态势指挥台通过PC端展示宁波电子政务外网政务终端信息，包含按不同业务系统角度分析展现主机资源运行情况，主机资产、主机分布、主机运行告警、主机脆弱性、主机安全事件、主机工单等。

浙政钉移动端为用户展示宁波电子政务外网的终端总数、整体资产的脆弱性等级统计及分布情况、终端面临网络安全事件总数及TOP的网络安全事件类型等信息。

* + 1. **数据安全指挥台**

数据安全指挥台支持在PC端和浙政钉移动端展示当前政务云环境下数据安全态势信息，综合展示数据安全以及数据库审计等信息。包括数据安全设备资产数量和变化趋势、风险事件统计分析、风险数据库、审计数据库操作等功能。

对用户管理范围内数据库的各类操作行为的监控和记录，可审计所有来源，涵盖所有访问数据库的路径、数据库操作行为，并记录详细的用户行为信息，包含如登录审计、访问审计、危险攻击、漏洞风险等。

* + 1. **机房运行指挥台**

机房运行指挥台支持在PC端和浙政钉移动端展示宁波市行政中心信息化集中机房等相关机房（包括宁波市行政中心信息化集中机房非屏蔽区和发展大厦机房等）动环信息态势，机房运行指挥台集合市级资产台账信息，提供机房级容量统计和机房概览统计。

* + 1. **安全运营指挥台**

安全运营指挥台展示当前宁波市电子政务外网的安全运营工作数据，并提供协同指挥的能力，包含协同处置、通告预警发布等。包括各类协同处置工单数量、各类网络安全事件的分布情况、各类预警信息的发布及响应情况、各类网络安全应急事件处置及指挥调度情况等信息的展示。

* + 1. **运行监测指挥台**

运行监测指挥台通过与评估系统对接或手动填报等方式提供评估考核视角的数据监测与分析能力，分析并展示基于考核的各项指标参数评分及其变动情况。

浙政钉移动端展示各指标项的分析结果。

* + 1. **区县级驾驶舱**

根据项目总体规划，为10个区（县、市）和2个功能园区个性化设计开发区（县、市）政务网络数据安全一体化指挥系统领导驾驶舱，开发工作包括原型设计、UI设计、前端开发、后端开发、系统测试和联调等，支持区（县、市）及功能园区个性化需求定制。驾驶舱功能模块与领导驾驶舱一致，展示内容根据属地区分。

* 1. **业务驾驶舱**

业务驾驶舱，面向市县两级业务部门用户，以业务系统为核心，展示其所属的政务云资源态势，及更多指标详情，并展示工单信息，便于推动具体工作。同时支持PC端和浙政钉移动端。业务驾驶舱是主要从业务部门视角展示其相关的电子政务资产、运行状况和安全态势等，建设内容包括全局统览、云端运行统览、网络运行统览、应用运行统览、组织业务统览、网络安全统览、主机运行统览、数据安全统览、机房运行统览、安全运营统览和运行监测统览等11个应用场景。

* + 1. **全局统览**

全局统览面向市县两级业务部门用户，支持PC端和浙政钉移动端，展示其负责的电子政务业务范围内的多项整体监测结果，包含包含云端资源使用、主机运行状态、网络运行情况、应用运行情况、组织业务状况、网络安全风险、数据安全风险、机房运行状态、安全运营、运行监测等。

* + 1. **云端运行统览**

云端运行统览面向市县两级业务部门用户，以业务系统为核心，向其展示当前部门在云端资产的运行情况，提供详情分析，方便运营人员开展业务监测分析等工作。包括云端资产情况、云安全事件列表、事件查询、事件详情查看等功能。

浙政钉移动端的云端运行统览展示各局委办上云的系统总量，以及数量情况，展示云安全事件、工单响应处置等信息。

* + 1. **网络运行统览**

网络运行统览面向业务部门用户，支持PC端和浙政钉移动端展示，展示其所在部门的网络运行情况。按照网络运行情况维度进行统计；统计分析各业务部门的业务流量、网络质量、丢包率、网络连接数等信息。并对其进行风险评分，达到一定阈值，进行界面告警；展示各类指标TOP排名情况。

* + 1. **应用运行统览**

应用运行统览统一展示应用运行状态信息，支持在PC端和浙政钉端展示应用异常类型数据与异常类型分布；应用运行告警信息、应用运维工单情况、应用系统安全风险态势等。

* + 1. **组织业务统览**

组织业务统览以业务部门的视角，支持在PC端和浙政钉移动端上了解到本单位的各部门所拥有的业务系统，相关的业务系统在政务云上的运行状态及分布信息。包括统计分析组织业务维度的风险指标、安全事件详情、安全事件响应处置等指标情况。

* + 1. **网络安全统览**

网络安全统览展示所监测网络安全情况，包括网络安全风险等级评分、风险资产、失陷资产、风险资产等级分布、攻击源分布、威胁类型、发起外连资产数量、风险资产状态分布、主机漏洞、主机脆弱性资产、网站态势、网络安全事件列表等，支持地图上实时动态展示攻击状态。

浙政钉移动端的网络安全统览以攻击者和攻击行为两大视角展示各局委办的安全风险。了解攻击者IP、发起攻击次数、资产的影响范围、攻击手段的统计信息、攻击手段的详情等信息。

* + 1. **主机运行统览**

主机运行统览主要展示各业务部门相关主机设备及主机设备所处的运行状态。包括主机硬件、网络的状态、异常设备的统计分析、主机维护工单情况、主机设备存在的安全漏洞、弱点等指标新信息。

浙政钉移动端的主机运行统览展示本单位的主机状态，各类型的主机数量分布信息；以二维条形图展示近7天的活跃主机数量，主机运行的状态情况，以及主机正面临的安全威胁的TOP排名信息。

* + 1. **数据安全统览**

数据安全统览展示宁波政务云环境下的各业务部门的数据安全态势信息。包括数据库的风险评分、敏感数据统计、风险数量，资产与被访问身份的标签数据、访问量等，数据库的各类操作行为，用户行为信息等指标。

浙政钉移动端的数据安全统览展示数据安全风险状况、敏感数据信息、风险数量以及TOP资产信息等。

* + 1. **机房运行统览**

通过PC端和浙政钉展示各局委办的各自系统所部署的位置信息，机房运维信息等。包括动力环境状况、资产状况、运维情况、计划情况、值班情况、访客情况等各类信息。

* + 1. **安全运营统览**

安全运营统览关注当前安全运营状态，支持在PC端和浙政钉移动端展示，主要包含工单管理和通知预警两部分。

支持各类通用通报的反馈情况的统计查看，支持与其他业务应用进行数据对接。当监测到重要系统存在重大风险隐患，或产生重大网络安全事件时，根据谁使用、谁管理原则，通过移动运营工作台进行信息发布，责任单位按期反馈处置结果。

* + 1. **运行监测统览**

运行监测统览为业务部门提供绩效考核视角的自评估能力，支持用户手动填报相关指标参数，系统通过参数填报自动实现评分，浙政钉移动端支持展示评分结果。

* 1. **运营工作台**

运营工作台是管理各项具体安全运营工作，便于运营工作管理者能更高效、更快捷并更精准的做出管理决策和管理动作。主要围绕监测预警、分析研判、响应处置、溯源定位、报告归档以及日常运维、特殊时期保障等工作。PC端运营工作台包括资源管理、威胁管理、响应处置、协同运维、通报预警、事件管理、安全实战、供应链安全、系统管理和数据管理配置等10个应用场景。

浙政钉上的移动运营工作台主要涉及运维工作内容，虽然包括资源管理、威胁分析溯源和响应处置，安全预警、安全实战、供应链安全等内容，但相对PC端功能上有所弱化。

* + 1. **资源管理**

运营人员可通过该模块对宁波市电子政务外网中的资产进行确认，为资产的精细化管理提供数据支撑。把资产与业务相互映射并产生协同，使得运营人员能更快的了解到各自负责业务系统当前安全状态，并根据对应安全风险制定响应安全处置方案。当发现重大漏洞爆发时，基于服务器管理数据可快速定位受影响的系统、服务器等受影响的资产范围。

资源管理包括资产分类管理、资产发现管理、资产全生命周期管理、脆弱性管理和知识管理等功能。

* + - 1. **资产分类管理**

宁波市电子政务外网的资产，结合实际使用情况进行分类，不同类型的资产有不同的敏感性和重要性。资产分类管理包括组织管理、云管理、业务系统管理和资产类型管理等功能。

* + - 1. **资产发现管理**

资产发现管理包括资产主动探测、被动发现资产、资产人工上报、资产检索与定位、资产确认、资产删除和资产编辑等功能。

* + - 1. **资产全生命周期管理**

对资产的状态进行全生命周期管理，包括入库、出库、借用、维修、报废等状态，记录资产状态的修改情况。通过查看资产全生命周期的行为，可以对资产全生命周期状况了如指掌。

* + - 1. **脆弱性管理**

脆弱性管理包括多来源漏扫设备兼容、多源漏洞数据融合分析、脆弱性发现与检索、脆弱性分析、脆弱性处置和漏洞处置优先配置等功能。

* + - 1. **知识管理**

知识管理是针对宁波市政务信息化网络数据安全相关知识资源进行管理，包括情报管理和知识库管理功能。情报管理包括情报展示、威胁情报源管理、威胁情报库升级、情报修改、自定义情报管理和热点情报等功能。知识库管理包括分类管理知识库，规划、编制、发布、更新、审核、评估知识库，规划、设计，选择适当的知识库存储媒介、存储格式和存储方式等功能。

* + 1. **威胁管理**

威胁管理是通过规则配置、告警评分、规则任务、威胁狩猎、场景建模、分析溯源、全文检索和安全报告等功能，实现对威胁信息的管理和成果输出。

* + - 1. **规则配置**

系统基于内置或者市大数据局及平台运维人员自定义的规则，使用分类、关联、统计、聚合等算法对收集第三方的安全告警日志进行处理，实现日志的分组与聚合。提升告警的准确性，达到告警风暴治理的目的。

* + - 1. **告警评分**

告警评分内置对网络安全事件的关键参数进行分析、计算和综合，对事件的紧急程度和优先级进行评估和划分，也支持定义关键参数，支持定义评估指标，支持对指标制定相应的评价标准和权重。

* + - 1. **规则任务**

规则任务可以统一监测告警规则是否被触发成功，规则触发执行时间、开始时间、结束时间、执行花费时间、输出记录等内容。可以通过监测列表集中查看系统中主要触发哪些规则，验证规则的有效性。规则任务是指对系统中的行为、流量等进行检测和分析的任务，包括病毒、恶意软件、入侵和攻击、用户行为等。

* + - 1. **威胁狩猎**

根据攻击者或受害资产IP，对威胁进行溯源，采用威胁狩猎功能，快速确定攻击者对受害资产的影响，支持把分析过程加入狩猎报告，辅助管理员进行分析。

* + - 1. **场景建模**

场景建模模块基于大数据分析技术，构建场景式威胁分析模型，结合多场景下威胁分析需求，赋予安全分析人员可视化安全建模能力，帮助安全分析人员理解威胁，用于分析多种来源的告警与日志，发现和识别安全风险，如 DNS智能防护、DGA 恶意域名检测、业务访问信任度评估等。

场景建模提供模型模板，可以查看和使用系统已固化的场景模型，快速了解系统既有场景。场景建模主要操作流程为创建模型，编辑场景模型，模型执行的启动、停止与删除。场景建模具备模型运行态数据实时记录机制。

* + - 1. **分析溯源**

支持查看安全威胁事件的攻击时序关系、钻取分析原始日志与相关日志、查看原始payload字段、查看威胁事件涉及的资产详情及脆弱性信息等并生成快照。支持创建分析溯源报告。。

* + - 1. **全文检索**

实现安全数据的多条件组合，选取关键字查询，按时间段、地址范围、数值范围不同字段值快捷生成可编辑条件进行搜索，实现字段值逐级钻取，支持搜索结果导出。可以执行模糊查询、精确查询、组合查询、批量查询、二次检索和查询结果导出等。

* + - 1. **安全报告**

安全报告功能模块可以生成安全日报、安全周报、安全月报、安全运营报告和应急处置报告等多种类型的报告。支持对报告模板进行编辑修改，从而输出新的报告。

* + 1. **响应处置**

响应处置包括处置任务管理、处置流程管理、剧本预案关联、剧本编排、处置待办、执行历史、响应通知和响应处置监控与优化等功能。

* + - 1. **处置任务管理**

处置任务管理是指针对网络安全事件的自动化处置任务进行管理和控制，包括任务的分配、执行、监控和结束等环节。

* + - 1. **处置流程管理**

处置流程管理是对处置流程的节点进行管理，支持对处理流程的编辑、发布、创建等。

* + - 1. **剧本预案关联**

剧本预案关联是安全告警与自动化剧本关联的桥梁，针对系统检测发现的各种安全告警与威胁事件，提供对应的响应处置关联策略，减轻安全运营人员的工作压力。支持根据告警类型设置预案剧本，满足条件时触发运行剧本。支持展示告警类型与剧本的关联信息。支持查询剧本执行状态。

* + - 1. **剧本编排**

通过该模块编排所属业务部门或区（县、市）安全剧本，包括自动封堵、自动查杀、自动部署虚拟补丁等。包括剧本编排的可视化设计功能，支持拖拉拽及其它相关操作，支持选择应用动作、API等元素，还包括剧本标签、剧本测试、剧本发布、权限管理、版本管理、剧本热加载等功能。

* + - 1. **处置待办**

处置待办是指通过本系统的剧本自动化响应处置系统自动或人工生成的待处理任务。

* + - 1. **执行历史**

集中展示所有安全告警自动化处置的情况，展现剧本运行状态、耗时等属性信息。

* + - 1. **响应通知**

支持通过SOAR的自动化能力，通过消息通知类的剧本，或者剧本中的消息通知语句，将剧本中网络安全事件相关的信息，通过短信、浙政钉等方式通知对应责任人员。

* + - 1. **响应处置监控与优化**

监控到每一个流程流转环节所涉及的操作以及每一个流程操作的耗时时间和调用次数。支持查看详情，支持多维度的排序，支持优化处置流程。

* + 1. **协同运维**

协同运维模块主要是提供各类安全问题的工单管理能力。协同运维包括工单管理、扫描测试报备管理、工单信息展示、工单对接、工单流转、工单权限工单流程模板、流程编辑和流程节点库等功能。

* + - 1. **工单管理**

本系统的工单主要来源三个方面：一是网络安全协同管理平台产生的工单，二是系统中运行，网络安全事件对应的工单，三是业务部门日常工作需要所建立发布运维工单。工单管理主要包含工单来源、工单来源分类、工单优先级设置、工单信息记录和我的工单等功能。

* + - 1. **工单信息展示**

工单信息展示可以帮助用户更好地了解和管理事件的处理情况，快速定位问题，提升工单处置效率。展示当前工单信息，包括但不限于：所属系统、所属组织、工单类型、工单处置率，工单趋势、工单处置效率等。

* + - 1. **扫描测试报备管理**

政务外网市级接入单位和各区（县、市）大数据中心会按需开展对本部门（地区）政务外网的漏洞扫描或渗透测试。扫描测试需提前向省、市大数据局报备，便于政务外网统一管理，同时避免引起误封。支持下到上以工单形式提交扫描测试申请，支持对扫描测试报备工单实行审批、查询、统计、管理和事件自动化匹配等。

* + - 1. **工单对接**

工单对接是系统与网络安全协同管理平台对接。工单对接内容包含工作内容描述，完成该项工作的人，以及工单的流转和完成状态等。支持对接网络安全协同管理系统，由平台工单系统执行工作任务的派发、工单的流转等任务，并将工单执行的任务状态反馈给网络安全协同管理系统。

* + - 1. **工单流转**

支持工单处置流程配置，通过可视化节点实现工单流转流程图的设计，包括对配置处理人或者处理组的配置，以及工单的流程节点配置。支持工单驳回、转派、审核、关闭流转动作。

* + - 1. **工单权限**

根据不同的处置权限添加对应的用户或用户组，使每个流程节点都可以与对应的用户或用户组进行绑定，实现对工单全流程的编辑定义。

* + - 1. **工单流程模板**

内置工单流程模版，支持基于工单流程模版来生成新的流程；工单流程模板支持编辑、删除等常见管理操作。

* + - 1. **流程编辑**

支持对安全告警处置工单流程编辑；支持拖拽流程图中节点（操作、判断、开始/结束）、连线、子流程、对象等。

* + - 1. **流程节点库**

提供预置的流程节点库，其包含多种类型的流程节点，如开始节点、分支节点、执行节点、审批节点、结束节点等。

* + 1. **通报预警**

通报预警根据接收到的监管部门、上级部门发布的消息，以及本系统发现的安全漏洞、木马、僵尸网络、暗链、APT攻击、DDoS攻击等安全隐患或事件，根据预定义的通报模板和预警策略，生成预警通报。通报预警包括通报总览、事件通报、公告管理和通知历史等功能。

* + - 1. **通报总览**

通报总览直观展示各区（县、市）及各业务部门的通报情况；支持对通报信息总览，内容包括事件通报信息汇总、公告管理和通报历史记录管理。

* + - 1. **事件通报**

将“我发送的通报”、“我收到的通报”和“抄送我的网络安全事件通报”进行统一汇总，可查看通报的事件信息。

* + - 1. **公告管理**

公告管理主要是针对监管部门、上级部门等部门发送的政策法规、安全隐患公告等；公告管理支持公告信息提示，并支持公告信息详情查看。

* + - 1. **通知历史**

通知历史可以帮助用户更好地了解事件的处理过程和情况，快速定位问题，加快解决速度；支持查看通报历史记录信息。

* + 1. **事件管理**

事件是基于数据资源层采集各类设备的日志，经过日志的解析、标准化、分析、关联等处理形成各类事件，事件管理包括事件列表、事件统计、事件筛选、事件归并、事件告警、事件处置建议、事件详情和事件检索等功能。

* + - 1. **事件列表**

事件列表可以帮助用户更好地了解整体安全风险状况，及时发现和处理故障、异常和安全的网络事件，提高系统稳定性和可靠性。包括事件型、描述、级别、处理状态、处理人员和处理结果等信息。

* + - 1. **事件统计**

支持图表和报表等多种方式统计事件数据的分布、趋势和规律；支持统计网络安全事件TOP5、网络安全事件类型饼状图、网络安全事件数量趋势图、当前热点网络安全事件等。

* + - 1. **事件筛选**

支持筛选网络安全事件相关的数据和信息。

* + - 1. **事件归并**

支持基于网络安全事件类型、网络安全事件关联度、网络安全事件风险度等条件进行事件归并，达到网络安全事件更精准效果，降低事件误报率。

* + - 1. **事件告警**

事件告警分为网络告警和终端告警。支持统计分析全网中发现的告警总数、受害者数量、攻击者数量、告警的种类等信息，支持事件信息多条件查询，运维人员针对展示出的告警信息可以发起工单、确认、加白、封堵等操作。

* + - 1. **事件处置建议**

事件处置建议可以帮助用户更好地解决事件，提高事件的处理效率和质量。可以快速定位问题、采取相应的措施进行处理，并从根本上解决问题，提高系统的安全性、稳定性和性能。支持制定符合当前宁波政务信息化网络环境的安全处置建议；支持筛选事件类型条件查询处置建议库建议，支持自定义编辑处置建议库信息。

* + - 1. **事件详情**

事件详情不但可以帮助用户更好地了解网络安全事件的情况，快速定位问题，采取相应的措施进行处理。也可以展示各业务系统运行情况，及时发现并解决问题，保证业务系统的稳定性和安全性。针对事件详情进行展示。支持运维人员“发起工单、确认、忽略、封堵”等操作。

* + - 1. **事件检索**

系统提供检索入口对网络安全事件进行查询，事件检索按照规则分类背后的正则逻辑提供检索条件。规则类型包括标准规则、分组规则、关联规则、序列规则。对于网络安全事件关联的IP地址、URL等支持下钻到关联的威胁情报和资产信息。

* + 1. **安全实战**

安全实战是针对安全演练、应急响应及重大安全保障活动期间的政务信息化网络安全防护工作，包括指挥调度、活动任务管理、值班人员管理、报告管理和预案管理等功能。

* + - 1. **指挥调度**

在重要会议或重大活动（重保、应急演练等）期间，加强网络运维人员指挥调度，全方位全天候掌握与活动相关的单位、系统和网站安全状况，及时通报预警网络安全隐患；支持对指挥调度、活动任务管理、值班人员管理、报告管理和预案管理维护。

* + - 1. **活动任务管理**

活动任务管理是针对安全演练、应急响应及重大安全保障等活动，确认活动任务、活动任务的分派、活动任务的跟进及反馈等。包括创建安全保障任务、任务分配、任务报告和归档。

* + - 1. **值班人员管理**

值班人员管理模块能够加强网络运维人员的调度，能够全方位全天候掌握与活动相关的单位、系统和网站安全状况，能够及时通报预警网络安全隐患，高效处置网络安全事件。值班人员管理包括记录和维护值班人员的基本信息、管理值班计划和排班表、监督和考核值班人员的工作等。

* + - 1. **报告管理**

报告管理模块可以帮助各业务部门了解自身的网络安全情况，及时发现和解决安全威胁，提高系统的稳定性和安全性。报告类型包括攻防演练实战报告、重保报告等；报告管理支持以报告名称维度统计报告信息，支持查看、报告导出等操作。

* + - 1. **预案管理**

为科学应对网络信息突发事件，建立健全应急响应机制，有效预防、及时控制和最大限度地消除信息安全各类突发事件的危害和影响，系统具备对应急响应预案的管理能力。预警管理维护支持预警时间名称名称、预警类型、发生时间、处置状态、负责人等信息。

* + 1. **供应链安全**

供应链安全是对宁波市信息化成果供应链厂商信息和安全进行监管，包括供应商管理、供应商软件组件管理、历史供应链数据查询和供应链风险管理等功能。

* + - 1. **供应商管理**

通过该功能对市县两级各部门的供应链进行管理，加强对供应链整体安全的管控；系统管理员或者指定账号支持对供应商信息做新增、编辑、删除的管理操作。

主要是供应商和风险进行管理，包括人员管理、项目管理、供应商评价、历史数据查询和分析、风险管理等。

* + - 1. **供应商软件组件管理**

供应商软件组件模块支持信息查询、标准模板信息导入、内容编辑、删除的管理操作。

供应商软件组件清单包括供应者名称、组件名称、组件版本、依赖关系等信息。该清单数据应符合SPDX 标准。

供应商软件组件管理模块支持授权、更新、修改、增加等功能。

* + - 1. **历史供应链数据查询**

历史供应链中支持对供应商的名称、项目名称等进行关联查询、支持历史供应链流程关联及关联查看。

* + - 1. **供应链风险管理**

支持调用漏扫等采集探针的扫描结果和有关的 0day 漏洞事件，对供应链上厂商负责的资产设备，进行潜在的风险与暴露面扫描，包含漏洞、端口、合规、弱口令等信息，并对其进行风险管理，对发现的问题，及时以站内信或短信的方式，提醒各业务部门及相关供应链厂家，及时修复对应漏洞、端口、合规、弱口令等潜在风险。

供应链风险管理中支持按照供应链信息综合查询、供应链风险结果的报表导出等操作。

* + 1. **系统管理**

系统管理是系统管理员通过统一监控、统一配置、菜单管理、消息管理和可视化管理，对系统运行进行相关的配置和监控；可以监控系统的状态和运行情况，系统的负载和性能指标等。

* + - 1. **统一监控**

统一监控展示系统运行监控、进行监控、采集监控、处理监控和系统日志等。

* + - 1. **统一配置**

统一配置主要用于提供一系列配置选项，允许系统管理员对系统进行管理。支持设置分析模型，选择合适的算法和模型结构。支持定义IP或IP段所属地区、所属国家等，支持添加多重逻辑组，选择模糊或精确查询等。

* + - 1. **菜单管理**

对系统菜单的设置、维护、修改和删除等操作，来实现系统菜单的管理工作。

* + - 1. **消息管理**

消息管理涵盖系统内部消息、即时消息管理、滚动消息、短信消息管理、浙政钉消息通知管理，主要作用是实现本系统内部消息管理和与第三方系统的消息交互管理。

* + - 1. **可视化管理**

可视化管理是为系统提供海量数据实时在线分析服务，包含图表、文字、图片、地图、指标等多种元素，可视化管理功能包括可视化编辑环境、数据配置、参数配置等。

支持对海量数据实时分析；支持拖拉拽的方式将模块放置到画布上，画布支持调整模块位置；支持预览效果；支持对关联的数据源和检索条件进行配置；支持对位置、大小、比例等可视化参数进行细致的配置。

* + 1. **数据管理配置**

数据管理配置包括数据源配置、数据处理配置、数据存储配置和采集任务配置等功能，以便适配用户需求。

* + - 1. **数据源配置**

支持配置数据源的接入信息，包含一键接入和数据接入功能，完成数据源的快速接入以及对应的采集周期设置;支持采集安全日志、网络日志、终端日志、系统日志等多种数据源;支持Syslog、SNMP、HTTP、JDBC、FTP、SFTP等多种采集方式。

* + - 1. **数据处理配置**

数据处理配置包括预处理任务、预处理模板、标准日志模板、数据解析和组件管理等配置功能。

* + - 1. **数据存储配置**

支持对日志、告警、事件、资产、情报等均可设置独立的数据存储周期。支持不同类型的数据存储节点，支持对不同类型数据的使用需求进行个性化配置，根据不同的数据类型或来源，可以定义不同的独立数据存储类型、保留时间等参数。

* + - 1. **采集任务配置**

支持对采集任务的新建及配置编辑等操作。

* 1. **应用支撑层建设**

为满足本项目运营管理门户数据统计、分类、展示和各项业务功能，建设通用组件和系统引擎。

* 1. **通用组件**

采用微服务架构构建通用组件，包括资产模型组件、权限管理组件、集群管理组件、系统管理组件、情报对接组件和身份体系验证组件等6个组件。

* + 1. **资产模型组件**

资产模型组件是对宁波市电子政务外网中的资产进行全生命周期管理，为业务应用层的资产管理功能提供数据支撑，资产模型组件包括资产属性管理、模型变更记录、模型属性查询和资产模型管理等。

* + - 1. **资产属性管理**

对资产属性，可以通过管理接口，进行调整，对其进行增删改的操作，以适配资产管理需求和资产特征的变化。

* + - 1. **模型变更记录**

系统对资产模型进行的改动，自动生成变更记录，包括修改内容和操作用户信息，便于后期进行确认和管理。

* + - 1. **模型属性查询**

支持对资产模型属性的查询;支持使用单关键字或多个关键字的条件组合，查询资产模型属性和详细信息。

* + - 1. **资产模型管理**

对资产模型进行管理。包括资产模型的新增，现有资产模型的基本属性修改，也可以删除资产模型。系统对资产模型管理操作，并生成变更记录。支持模型、属性的导入和导出功能。

* + 1. **权限管理组件**

权限管理组件是对于系统的权限基于角色进行管理，为不同角色的用户权限调整提供支撑，权限管理组件功能包括权限模型、权限管理模块、系统角色管理、授权管理等。

* + - 1. **权限模型**

用户对系统访问权限分为数据权限、功能权限、操作权限，其中数据权限代表用户在系统上有权查看的数据范围，通过关联的资产、设备限定；功能权限代表用户在系统可以访问的功能界面范围；操作权限为用户在系统上所能执行的操作类型范围。

* + - 1. **权限管理模块**

权限管理模块提供配置界面、授权模块、鉴权模块。配置界面支持管理员在界面进行用户账号管理、权限域管理、账号权限分配等管理操作；授权模块提供接口供组件注册权限项，支持界面进行授权配置，资产设备相应权限信息与资产、设备管理模块进行联动；鉴权模块提供接口供其他组件和界面进行用户身份认证以及功能、操作、数据鉴权。数据权限与资产、设备管理模块进行联动。

* + - 1. **系统运维角色管理**

系统数据权限和功能权限的管理，都是基于角色来定义。通过设立不同的角色，对角色设置不同的权限，可以实现不需对具体的人员进行独立授权，批量授权的目的。

* + - 1. **业务角色管理**

业务角色管理结合组合架构、业务需求和工作流程进行分析和设计，通过角色分析确定各个业务角色需要的系统权限和操作，将其绑定到角色身上，并进行分配和授权。同时，通过对角色进行管理和调整，保证业务操作的连贯性和一致性。

* + - 1. **授权管理**

对于数据权限和功能权限的授权，根据不同角色，设置其数据访问权限和功能使用权限，也支持按角色组进行配置。授权管理，一般只有管理员能进行操作，同时系统记录操作日志。

* + 1. **集群管理组件**

集群管理组件包括节点管理、运行状态监控、集群配置、故障转移恢复、集群控制等功能。

* + - 1. **节点管理**

支持管理集群主节点和各工作节点，支持配置节点基本信息，可以按需进行调整工作节点。

* + - 1. **运行状态监控**

支持按集群结构监控主节点及各工作节点的运行状态。支持设置节点运行状态异常规则，对集群主节点及各工作节点的运行异常状态进行告警。

* + - 1. **集群配置**

支持配置和修改集群基本配置参数，以及各种运行控制参数。

* + - 1. **故障转移恢复**

当集群中某个工作节点运行故障时，集群会启动故障转移机制，自动转移工作负载到其他备份工作节点，并将原节点的负载任务恢复运行，从而避免负载任务的中断。

* + - 1. **集群控制**

支持集群控制管理，包括但不限于启动、停止、重启和查看操作。

* + 1. **系统管理组件**

系统管理组件是为系统正常运行提供支撑，系统管理组件功能包括系统信息管理、菜单管理、升级管理、用户管理、系统监控、审计管理、系统参数、许可管理、故障管理等。

* + - 1. **系统信息管理**

支持管理名称、Logo、登录账户、文件服务器、NTP服务器等。支持对各种服务器的设置，包括主机IP、端口、服务参数等配置。

* + - 1. **扩展菜单管理**

支持不同角色用户对菜单自定义扩展的管理和配置变更的记录；支持定制化的操作，对系统中已有的扩展进行维护和修复，包括删除无效的扩展、修复已有的扩展。

* + - 1. **升级管理**

支持在线和离线两种方式升级平台版本。支持升级过程回滚，如果升级失败，可以回滚到升级前版本。

* + - 1. **用户管理**

提供对用户进行新增、修改、删除等操作。支持为所有可访问的页面和接口提供专用的登录控制模块对登录用户进行身份标识和鉴别。

* + - 1. **系统监控**

支持监控组件的运行情况，记录各组件中资源使用情况、模块运行情况、软件访问情况等信息。

* + - 1. **审计管理**

支持记录用户所有的系统操作信息和状态，具体展示内容包括：用户名、IP地址、描述、操作状态、操作结果、创建时间。

* + - 1. **系统参数**

系统参数提供本系统其他基础配置管理能力。包括内网IP配置、网络适应能力和配置备份。

* + - 1. **许可管理**

系统自身软件和组件的许可管理，管理员能够查看系统和组件的状态和使用期限。支持对功能和组件的启用、停用等操作。

* + - 1. **故障管理**

支持高可用方式实现冗余存储、负载均衡，并设计其故障告警模块。

* + 1. **情报对接组件**

情报对接组件是实现多源情报数据的汇聚和接入，本地接入包括厂家报送的情报信息、第三方收集报送的情报信息、上级部门下发的情报信息、下级报送的情报信息以及通过其他模块汇聚的情报信息。情报对接组件包括情报对接、情报分析、鉴定引擎管理、白名单管理、对接状态监控、威胁情报统计、情报新增与导出等功能。

* + - 1. **情报对接**

情报对接包括情报采集、情报处理和情报展示层等功能。

* + - 1. **情报分析**

指导各分析引擎在情报碰撞过程中，自动留存高价值情报信息，便于安全运营人员在查询分析结果；平台通过对情报信息的处理，对无用的情报信息进行清洗处理；上层关注高价值的情报信息，为安全运营人员提供处理依据。

* + - 1. **鉴定引擎管理**

鉴定引擎管理用于对样本分析相关功能进行配置调整，进而指导样本分析引擎对恶意样本分析的严格程度。

* + - 1. **白名单管理**

白名单管理功能模块支持分别对全局白名单、情报白名单进行管理，支持有权限的业务人员或运维管理人员对白名单进行增加、删除、修改等操作。

* + - 1. **对接状态监控**

支持通过监控对接状态，掌握对接组件状态，若出现异常，可及时人工干预。

* + - 1. **威胁情报统计**

支持多维度统计各情报源获取的威胁情报数据，包括但不限于来源、情报类型、情报置信度。

* + - 1. **情报新增与导出**

支持人工新建或导入情报信息，时刻丰富情报管理内容，关联掌握最新的情报信息。

* + 1. **身份体系验证组件**

身份体系验证组件是一种用于验证用户身份的软件组件，可以使用不同的身份验证方式来确保只有经过授权的用户才能访问系统或资源。身份验证组件包含用户认证管理、身份管理、会话管理和安全审计。

* + - 1. **用户认证管理**

对接浙政钉满足用户浙政钉用户扫码登录需求。支持账号密码和验证码等其他验证方式。支持账号密码或者浙政钉扫码登录，等其他凭据时来访问宁波市政务信息一体化网络数据安全一体化指挥系统，系统支持对比用户提供的凭据与保存的是否匹配。

* + - 1. **身份管理**

支持结合浙政钉的身份管理体系，实现数据平台4A级统一安全管理。支持浙政钉实现基于角色访问权限控制，通过系统给用户或用户组赋予角色的方式进行用户权限管理。支持结合权限的管控，通过统一的分布式存储HDFS的文件以及目录权限管控，实现数据隔离。支持通过统一的计算资源调度管理框架YARN的作业与队列的权限管控，实现计算资源的隔离支持通过对于数据仓库的数据库、表、视图的权限管控，实现统计分析以及数据挖掘的管控；支持通过对于实时在线数据库的表、行、列、单元格的权限管控，实现数据检索以及即席查询的管控；支持通过对于实时数据流的创建、删除、读取以及写入的管控，实现实时流处理业务的数据隔离与管控。

* + - 1. **会话管理**

跟踪用户的活动并保持用户会话的安全性。支持为每个会话分配唯一标识符。支持Cookie、Session验证用户登录及其操作的合法性。支持监控无非法注入、跳过重要步骤、恶意攻击行为发生，通过记录、检查日志等异常问题。

* + - 1. **安全审计**

支持应用系统行为安全的审计与管理功能。支持对所有系统操作进行精细化管理，支持审计所有操作记录流水的记录、存储、查询与统计。审计日志包含用户记录、时间记录、操作记录、数据记录。支持统一的审计日志查看界面，审计员角色拥有该页面权限。支持审计日志的查询和导出功能。

* 1. **系统引擎**

系统引擎主要作用是为上层业务应用做技术支撑，主要包括指标管理引擎和报告生成引擎。

* + 1. **指标管理引擎**

数据源管理主要功能是对指标数据源数据库进行初始化配置管理为后续创建指标接口提供数据服务。指标管理引擎功能涵盖数据源管理、安全指标管理、安全指标监测、安全指标接口和指标搜索配置等。

* + - 1. **数据源管理**

支持管理指标来源、指标阈值、指标来源单位、指标更新频率、指标标签等，支持新增、编辑、查询各种安全指标数据。

* + - 1. **安全指标管理**

安全指标管理主要用于新增、编辑、查询各种指标数据，针对驾驶舱各个主题屏、专题屏的指标来源、指标阈值、指标来源单位、指标更新频率、指标标签等信息，进行查询、指标清单导出、指标接口的创建。

提供指标列表，支持多条件、模糊指标查询。指标支持一键导出为指定文件。支持将选中指标添加到指定场景。支持创建指标，支持从指标列表中单个或批量删除指标。支持创建接口。支持指标下架。支持指标替换。

* + - 1. **安全指标监测**

安全指标支持设定预警阈值，阈值内容至少包括业务阈值、报警阈值，支持根据设定的阈值进行监测预警，并支持关联到指标。

* + - 1. **安全指标接口**

指标管理引擎预留安全指标数据调用接口，支持安全指标数据调用接口，供其他应用调用。

* + - 1. **指标搜索配置**

支持在指标列表配置多维度热门指标，如最多搜索、最近上架、近期报警。支持配置完成的指标展示在高级搜索中，可以快捷的查看和使用。

* + 1. **报告生成引擎**

报告生成引擎内置富文本功能模块和多种数据分析模型，可按照指定周期，提供多样化数据分析，生成图文并茂、数据精确、详细的各类型数据分析报告。

* + - 1. **报告模板管理**

支持模板的管理功能，包括模板新增、编辑、查看、删除。支持报告模板相关的多种表格、饼图、柱形图、折线图、条形图、地图、散点气泡图、漏斗图、日历图等素材管理。支持模板审核，仅审核通过的模板允许添加到模板库。支持模板库功能，提供通过审批的模板供参考，支持查看和使用。

* + - 1. **智能报告管理**

系统报告生成引擎中支持选定报告模板手动、自动方式生成，支持以图文方式的结果输出。支持自动报表生成。支持手动报表生成。支持多维度的模式切换查看报表信息，支持基于报表信息查询指定的报表。支持docx、pdf的格式报表导出。支持基于报表信息查询指定报表。

* 1. **数据资源层建设**

数据资源层是为业务应用层和应用支撑层做数据服务，包括分析引擎、数据库、数据治理、接口管理和第三方威胁情报对接等。

* 1. **分析引擎**

通过数据资源层对原始日志解析成标准日志，在通过分析规则生成可疑告警，经过关联分析引擎和告警归并引擎生成准确、有效的网络安全事件。分析引擎包括规则分析引擎、关联分析引擎、告警归并引擎、智能分析引擎和融合建模引擎等。

* + 1. **规则分析引擎**

规则分析引擎用于分析和处理规则，可以自动化地执行规则，通过系统与数据源集成，帮助系统更好地管理和优化业务流程。规则分析引擎包括规则设置、规则分析、结果输出、黑白名单管理和规则库管理等功能，建设的引擎包括流量检测引擎、资产分析引擎、情报分析引擎、样本分析引擎、语句封装引擎、流计算引擎、批计算引擎、分布式计算引擎、分布式检索引擎等。

* + - 1. **规则设置**

支持设置的步骤包括选择规则类型，设置判断逻辑、制定规则策略、输出配置，告警归并。

* + - 1. **规则分析**

支持基于多个维度查询网络安全事件和漏洞事件（自定义指标），以及基于时间维度关于攻击行为的呈现，支持以时间轴的形式展示在不同时间段内，攻击者攻击环节的评估，以此评估攻击的破坏性和影响性。

* + - 1. **结果输出**

支持分析后的结果输出到指定的数据库、文件、Web服务。

* + - 1. **黑白名单管理**

支持对IP加白、加黑等操作，实现对误告警的过滤和对重点告警的关注。支持黑白名单的新建、导入、导出、删除、查询、信息编辑功能。

* + - 1. **规则库管理**

分析规则库含一系列安全分析规则，这些规则可以检测出网络中可能存在的安全威胁和漏洞，从而及时发现和应对安全问题。通过管理和升级规则库来获取已知特征码或恶意IP等网络安全事件信息。为满足不同的场景，支持对规则重新定义分组、启停、自定义等管理操作

* + - 1. **流量检测引擎**

支持深度包检测、流量统计分析、特征识别及规则检测等方式。支持非法外联、违规操作、木马通讯、异常DNS、DDOS攻击、异常HTTP访问、蠕虫肉机等网络威胁进行检测和分析。支持深度解析流量元payload字段，可发现主流常见网络流量威胁。

* + - 1. **资产分析引擎**

支持统计学、机器学习、人工智能等方式把威胁感知发现的网络安全事件或安全威胁与部内资产进行关联分析。支持分析影响资源的分布以及受影响的关键特征。支持对风险点的修复情况进行跟踪。该系统还将结合资产信息、所监测到的脆弱性信息和威胁信息对资产进行风险评估。

* + - 1. **情报分析引擎**

支持提取多维度高可信威胁情报IOC关联安全日志和流量，可实时检测出恶意攻击，并根据情报的威胁分值设定相应的威胁等级。支持威胁类型、恶意家族、APT组织、可信度、危害等级、杀伤链、标签等多维度信息。支持海量日志、流量等元数据与情报信息进行碰撞，发现潜在的风险。支持日志、流量、告警等元数据溯源取证、对网络安全事件进行研判分析及响应处置的过程中随时调取元素的情报信息。

* + - 1. **样本分析引擎**

支持终端和流量提交已知样本文件MD5进行查询，实现毫秒级查杀响应。支持以图表、报表等形式展现出来，方便用户进行数据理解和决策。支持将样本分析结果与其他系统进行集成和关联，如情报库、业务组件等。

* + - 1. **语句封装引擎**

语句封装引擎在本系统中核心用于实现安全风险的自动化/半自动化响应，引擎预留丰富的调用接口，用于实现与各类具备联动条件的第三方应用进行联动。

* + - 1. **流计算引擎**

系统基于流处理技术构建分布式实时流计算引擎来解决实时流式数据处理。通过流计算引擎，可以对数据流进行有状态的计算。

* + - 1. **批计算引擎**

构建分布式批计算引擎，提供通用灵活的DAG多轮批计算模型，在此基础上提供处理海量结构化数据的SQL接口，对数据做深度分析以及集群学习算法。

* + - 1. **分布式计算引擎**

支持集群节点之间共享数据的能力。支持集群节点之间调度作业的能力。

* + - 1. **分布式检索引擎**

支持实时分析的分布式搜索引擎，处理TB级别的结构化或非结构化数据。

* + 1. **关联分析引擎**

关联分析引擎是一种数据挖掘工具，用于发现数据集中不同变量之间的相关关系，促进平台掌握数据集中的规律和趋势，从而做出更好的展示以及帮助用户做出更好的决策。平台内置多种关联分析引擎类别，包含数据处理、事件聚合、数据关联等引擎内容，更好的支撑整体平台数据分析与展示。

* + - 1. **数据预处理模块**

数据预处理是指在对数据进行数据挖掘的主要处理以前，先对原始数据进行必要的清洗、集成、转换、离散、归约、特征选择和提取等一系列处理工作，达到挖掘算法进行知识获取要求的最低规范和标准。

* + - 1. **关联规则挖掘模块**

该模块用于从数据集中挖掘出具有一定置信度和支持度的关联规则。

* + - 1. **可视化模块**

将挖掘出来的关联规则以图表的形式展示，使用户更容易理解数据之间的关系。

* + - 1. **事件聚合引擎**

本系统通过设计事件聚合引擎，可辅助安全运营团队完成网络安全事件聚合还原分析工作。安全场景规则使用事件聚合引擎，以告警为入口，把安全分析人员手动的分析溯源过程用模型的能力实现，将多个告警和日志进行上下文自动校验和关联，聚合成为一个具体的网络安全事件。

* + - 1. **多维数据关联分析**

多维数据关联分析包括基于IP地址的关联分析，基于时间维度的关联分析，基于用户行为的关联分析、基于安全漏洞的关联分析和基于特定文件的关联分析等内容。

* + - 1. **关联模型评估**

关联模型评估是指对已生成的模型或场景进行评估，验证模型或场景的准确度、可用度等。

* + - 1. **数据预测模块**

数据预测模块是关联分析引擎中的一个重要组成部分，它主要用于利用历史数据或已知规律对未来数据进行预测。数据预测模块可以根据数据类型的不同，支持ARIMA、SARIMA以及LSTM算法；支持决策树、朴素贝叶斯、逻辑回归算法。同时可将关联规则应用于新的数据集，用于预测新数据之间的关系。

* + 1. **告警归并引擎**

告警归并引擎功能是将来自多个监控系统的告警信息进行归并和去重，从而减少冗余和重复的告警信息，提高告警的可读性和可管理性。

* + - 1. **告警降噪处理**

告警降噪的本质是将准确的告警按照亟需处理的级别进行排序处理。通过据源的可信度分析、白名单机制、冗余告警和重读告警的处理实现消除无效告警。支持调用威胁情报。对日志进行去重、去误、优先级排序、关联分析等优化处理，保留情报命中告警，实现海量告警的降噪处理。

* + - 1. **智能化处置**

支持正则匹配、关键词提取等以实现精准的数据分类和过滤，降低后续处理的运算量和时间，提高模型处理效率。支持基于已训练好的模型进行数据预测和降噪处理。

* + 1. **智能分析引擎**

依托宁波市政务外网、华为云、城市大脑已有的安全监控平台、安全设备的能力，并据此形成宁波市政务网络安全大数仓数据资源池，基于海量的安全数据和成熟的分析模型，建设适应宁波本地实际情况的智能分析引擎，补充市政务信息化网络数据安全事件一体化分析能力，进一步提升政务信息化网络数据安全监测预警能力。

智能分析引擎包括智能失陷主机分析、信息智能探测、暴力破解智能分析、账号明文传输检测、后门木马检测、主机挖矿检测、病毒扩散分析、僵尸网络检测、数据泄漏检测、账号共享检测、外联CC检测和会话风险检测等12项分析能力。

智能分析引擎主要通过采集多种网络协议的原始流量数据和服务器日志数据，通过基础的数据清洗、转换、聚合后，分析提取为设备、应用、数据和用户各实体的行为数据，为分析模型提供数据基础。

* + - 1. **智能主机失陷分析**

智能主机失陷分析通过分析主机访问情况判断主机是否已经失陷；支持任意数量聚合字段作为聚合对象。

基于历史行为数据，多维度挖掘实体关系，识别正常行为模式，建立正常主机行为基线。

支持基于规则的智能主机失陷分析，提供单一维度和多维度的主机行为异常分析。

支持基于机器学习算法的智能能主机失陷分析，提供不低于两种异常行为分析算法。

* + - 1. **信息智能探测**

支持基于攻防角度分析出攻击者在各方面信息探测行为进行分组和聚合统计特征，如端口扫描、漏洞扫描、目标遍历、URL拆解等。

支持长期数据训练学习，形成信息探测行为习惯模型，提供不低于两种学习算法。

支持分析过程中不断优化信息探测行为习惯模型，提供信息探测训练评分模型，对不同的行为进行评分，提高信息探测分析准确性。

* + - 1. **暴力破解智能分析**

支持在海量数据中根据暴力破解选取字段进行分组和聚合统计生成特征，包括访问时间、访问次数、访问频率、访问失败率等。

支持长期暴力破解分析，基于长期、低频等特征形成长期暴力破解行为模型，支持分析过程中不断优化，提高长期暴力破解分析准确性。

支持短期暴力破解分析，基于短期、高频等特征形成短期暴力破解行为模型，支持分析过程中不断优化，提高短期暴力破解分析准确性。

* + - 1. **账号明文传输检测**

支持基于账号是否使用哈希等加密算法进行单一维度的数据异常检测，根据账号数据是否匹配加密算法特征，判断是加密账号或非加密账号。

支持动态配置加密算法，可按需扩展账号匹配的加密算法特征内容。

* + - 1. **后门木马检测**

基于历史行为数据提取木马特征，多维度挖掘实体关系，识别正常行为模式，建立正常行为基线。

支持识别后门，支持长期数据训练学习，形成木马预期行为模型，通过攻击使用触发器的逆向工程，识别后门的预期操作。

支持检测后门，基于已经被后门感染且经过训练的数据模型，对输出标签进行错误分类，判断是否存在木马或变种。

支持策略模型级别实现实际安全威胁检测，定义在某个风险分区间为可疑、提醒、告警等检测结果标签，实现具体安全威胁场景的检测与落地。

* + - 1. **主机挖矿检测**

支持从网络中根据主机挖矿选取字段进行分组和聚合统计生成特征，包括识别矿机IP、矿池域名、矿池IP、当前所在的挖矿阶段、所挖的币种、采用的网络协议等信息。

支持长期数据训练学习，形成主机挖矿行为习惯模型，提供不低于两种学习算法。

支持分析过程中不断优化主机挖矿行为习惯模型，提供主机挖矿训练评分模型，对不同的行为进行评分，提高主机挖矿分析准确性。

* + - 1. **病毒扩散分析**

支持利用预处理后的海量数据建立推测病毒扩散模型所需的多维度特征，并按不同的字段从行为数据中提取特征，根据病毒扩散选取字段进行分组和聚合统计生成特征，包括病毒特征、时间范围、横向移动、病毒端口等。

支持配置条件前置规则，方便灵活实施流程控制逻辑；支持配置逻辑规则，能够定义灵活的、周期性的时间区间；支持配置运算规则，方便定义各种占比逻辑规则；支持配置调用指标，实时匹配数据特征 。

支持长期病毒扩散分析，基于长期、低频等特征形成长期病毒扩散行为模型，支持分析过程中不断优化，提高长期病毒扩散分析准确性。

支持短期病毒扩散分析，基于短期、高频等特征形成短期病毒扩散行为模型，支持分析过程中不断优化，提高短期病毒扩散分析准确性。

* + - 1. **僵尸网络检测**

支持安全威胁场景存在灵活多变的逻辑，规则内部须支持多种逻辑匹配模式（满足任意、满足所有、均不满足等）；规则内部条件支持单个条件与条件组，条件组可配置多种逻辑匹配条件。支持僵尸网络行为数据的学习，从行为数据中分析提取正常设备和僵尸机的特征，按多个维度分析挖掘实体间的关系，识别正常行为模式并建立正常行为基线。

支持长期深度网络流量学习，形成僵尸网络行为模型，提供不低于两种学习算法。将特征提取与模型训练过程结合，从全局的角度识别僵尸网络流量。

支持分析过程中不断优化僵尸网络行为模型，提供僵尸网络训练评分模型，对不同的行为进行评分，提高僵尸网络分析准确性。

* + - 1. **数据泄漏检测**

支持全网安全数据日志进行安全策略模型建模，识别关键威胁场景与数据流动场景，进行实时关联分析，捕捉数据泄漏行为。

支持数据波动异常行为场景，提炼短期内流量突增、短期内发送多个不同文件等威胁特征，建立异常波动策略模型，判断数据泄漏行为。

支持历史行为基线波动异常场景，识别当下的数据波动量与过去同时段对比，提炼若干这种威胁特征，综合判断数据泄漏行为。

* + - 1. **账号共享检测**

支持历史行为基线算法学习每个账号的常用设备、常用IP、正常行为模式，在通过关联算法经过比对，发现非常用设备、非常用IP、异地登录、异常行为序列等。

* + - 1. **外联CC检测**

基于历史行为数据提取外联CC特征，识别隐藏心跳行为，建立正常行为基线。

支持长期数据训练学习，形成外联CC行为检测模型，提供不低于两种检测方式。

支持分析过程中不断优化信息探测外联CC检测模型，提供外联CC训练评分模型，对不同的行为进行评分，提高外联CC检测分析准确性。

* + - 1. **会话风险检测**

支持异常访问模型的结果与会话漂移模型联合构造会话异常与会话窃取策略模型。

支持基于系统的实时指标模块提供的关联取值算子构建会话异常变化指标，识别会话漂移。

* + 1. **融合建模引擎**

融合建模是一个为用户提供自主数据挖掘分析建模的全面平台，它是基于大数据技术的产品，是集合大量统计分析功能、灵活配置规则、丰富而全面的数据分析方法与通用的机器学习算法的综合分析建模平台。

用户可以根据自身实际业务等方面的情况，有针对性去自主定义挖掘分析目标、探索数据、主动地去统计分析、自定义配置符合自身业务需求的规则、利用机器学习技术建立适应自身业务特性的数据模型、挖掘出数据中存在的巨大价值，为用户在场景建模、安全风险管控、业务分析、管理等方面，提供更加直观，更加有效的、更加迅速的建模分析能力。

* + - 1. **建模工作流程**

抽取分析场景开发共性特征，形成标准化的建模工作流程。

支持内置的多类分析模型，辅助用户设计场景模型，通过数据源引导、算法引导，选定场景模板、快速实例化安全分析场景。

支持前台拖拽的方式，调整合适算子模型，优化实例中的业务分析流程。

支持设计配置场景中所需算子的属性值，包括数据的输入、输出、计算方法等。

支持根据场景运行评估结果，通过场景逻辑优化，参数调整，实现模型的整体优化以及迭代。

* + - 1. **流程建模**

支持大数据处理架构，其中用到数据读取、数据分发的消息队列的技术，任务执行的中间状态数据使用内存分布式缓存，分布式计算框架作为离、在线任务的执行计算引擎。

* + - 1. **模型总览**

支持展示安全运营人员创建的场景和系统出厂默认的场景内容，通过场景的描述帮助安全分析人员快速、准确理解场景的内容和实现逻辑，实现内部运营场景和外部引入场景的模型知识的快速共享。

支持融合建模中各场景的运行状态，帮助安全分析人员实施监控各项任务运行情况，帮助其快速修复运行异常场景，保障融合建模中场景任务运行正常。

* + - 1. **模型管理**

模型管理包括新建模型、模型编辑和模型删除等功能。

模型管理能够提供系统核心的用户化安全场景建模能力，帮助用户通过安全分析场景的编排，实现场景的落地。具体功能包括数据流处理自定义功能、安全分析场景编排功能、多类型场景构建功能、多类型计算处理节点功能、输入算子、输出算子、处理算子、多分析算法支撑能力、分类算子、回归算子、聚类算子、模型训练能力等。

* + - 1. **模型任务管理**

支持通过场景名称和场景状态快速定位需要监测的在线场景运行任务并监测其执行情况。

支持以图形化的方式，展示离线场景运行状态和执行过程结果，并能够针对任务运行状态进行快速维护。

* + - 1. **行为异常模型**

支持机器人自动模仿人类用户的登录行为，以便检测和预防系统的安全漏洞和攻击。

支持账号短时异地登录模型是使用机器学习算法来识别和预测短时异地登录行为的模型。

* + - 1. **URL模型**

支持恶意URL地址加入黑名单，建议黑名单机制。

WebShell模型对WebShell的特征进行分析和建模，从而可以发现和预测系统中发生的可疑行为。

Web行为模型支持对用户访问的历史记录和交互数据进行收集、处理和分析。

* 1. **数据库**

数据库是通过数据分层和数据建模建设，形成系统相关的专题库。

* + 1. **数据分层**

系统数据架构构建贴源数据层、基础数据层、明细指标层和汇总指标层四个数据层。

* 贴源数据层：采用分布式行存储，做短周期的老化处理；同时采用消息队列进行临时缓存，供后续环节消费使用。
* 基础数据层：对数据进行清晰、补全、校验等标准化操作，形成结构化数据，根据数据量大小和特性选择存储方式。
* 明细指标层：在基础数据的基础上进行关联和轻度聚合，算出对应的指标，采用大数据库进行存储。
* 汇总指标层：在明细指标的基础上按照不同维度进行统计后的结果型数据汇总，采用列式存储或者关系型数据库进行存储。
  + 1. **数据建模**

数据建模包括范式建模和维度建模。数据建模应用于业务层的数据接入模型、分析数据模型、展示数据模型等，提高数据预处理、数据治理与开发、数据分享的效率。

* + - 1. **范式建模**

范式建模至少包含主题域模型和逻辑模型。主题域模型是业务模型的概念模型，而逻辑模型则是域模型在关系型数据库上的实例化。通过范式建模实现库表数据的获取，提供给上层应用，进行数据分析。

* + - 1. **维度建模**

维度建模能快速完成政务用户需求分析，支持运营工作台的数据快速查询，维度建模中表的类型至少支持事实表、明细表和维度表。维度建模支持星型建模、雪花建模和星座建模。

* 事实表：发生在现实世界中的操作型事件，其所产生的可度量数值，存储在事实表中。从最低的粒度级别来看，事实表行对应一个度量事件。
* 明细表：为分析方便，把事实表中的一个字段切割提取多个属性出来构成新的字段，因为字段变多，所以称为宽表，原来的成为窄表。
* 维度表：每个维度表都包含单一的主键列。维度表的主键可以作为与之关联的任何事实表的外键，维度表行的描述环境与事实表行完全对应。维度表通常比较宽，是扁平型非规范表，包含大量的低粒度的文本属性。
  + 1. **专题库**

建设包括电子政务资产信息库、网络安全事件库、供应链信息库、应用库、处置建议库、网络安全专家库、安全漏洞库、安全告警库、运行日志库、组织架构库、工单库、情报库、应急预案库、弱口令库、系统管理库、系统数据管理库、地理信息库和图表组件库等18个专题库。

* + - 1. **电子政务资产信息库**

电子政务资产信息主要包括IP地址表、IP地址变更记录表、电子政务资产类型表、端口信息表、设备类型表、重保资产表、责任人表、主机信息表、数据库表等。

* + - 1. **网络安全事件库**

网络安全事件库包括告警事件表、事件类型表和事件处置结果表等。

* + - 1. **供应链信息库**

供应链信息库包括供应商信息表、供应商人员表、供应商项目表、供应链产品表和供应商评价表等。

* + - 1. **应用库**

应用库包括应用责任人表、应用信息表和应用组件表等。

* + - 1. **处置建议库**

处置建议库包括处置建议表和处置类型表等。

* + - 1. **网络安全专家库**

网络安全专家库包括网络安全专家信息表、网络运维专家信息表、云平台专家信息表、操作系统专家信息表、数据治理专家信息表等。

* + - 1. **安全漏洞库**

安全漏洞库包括WEB漏洞表、系统漏洞表、中间件漏洞表、数据库漏洞表等。

* + - 1. **安全告警库**

安全告警库包括安全告警时间表、安全告警表和告警类型表等。

* + - 1. **运行日志库**

运行日志库包括登录日志表、操作记录表、云主机运行日质表、终端运行日质表、数据库运行日志表和机房运行日志表等。

* + - 1. **组织架构库**

组织架构库包括组织部门架构信息表、组织架构联系人信息表等。

* + - 1. **工单库**

工单库包括工单表单字段配置表、工单流程配置表和工单执行记录表等。

* + - 1. **情报库**

情报库包括恶意IP表、恶意DNS表、恶意URL表、热点情报表等。

* + - 1. **应急预案库**

应急预案库包括预案记录表、剧本表、剧本执行记录表、插件版本表和插件接口表等。

* + - 1. **弱口令库**

弱口令库包括弱口令记录表和弱口令加固记录表等。

* + - 1. **系统管理库**

系统管理库包括系统版本号表、系统配置信息表、功能权限信息表、数据权限信息表等。

* + - 1. **系统数据管理库**

包括基线违规表、基线整改记录表等。

* + - 1. **地理信息库**

包括行政区划表、市县两级电子政务行业监管部门/业务部门地址表、经纬度表等。

* + - 1. **图表组件库**

创建图标组件库，通过图标信息表、图标模型图，为两掌、领导驾驶舱、业务驾驶舱及本系统所有LOGO、图标进行图标支撑。

* 1. **数据治理▲**

本系统需要对接20多种类型的各个厂家的设备，含同种类型同一厂家的不同版本设备。按浙数局发〔2023〕2号文件附件7，对数字化改革重大应用的日志进行采集和归集，并需按照标准采集的数据进行清洗，以标准格式存储数据等。

* + 1. **数据采集汇聚**

数据采集汇聚包括数据接入一站式配置、采集实例通道和采集任务管理。全面支持常用采集协议，提供不少于11种采集协议下的数据采集能力；支持对不少于7家厂商28种设备（包括主机、网络设备、安全设备、应用、中间件、数据库）数据源的接入，并支持快速配置和联调实现新设备接入。

* + - 1. **数据接入一站式配置**

支持数据集成从数据采集、数据预处理到数据装载的一站式接入功能，提高系统的易用性，提高数据集成的效率。

支持数据集成的可视化编排，通过拖拽方式进行数据集成流程的构建，提高系统的可视化程度，降低用户的使用门槛和学习成本，有助于形成可复制、可传承的知识沉淀。

* + - 1. **采集实例通道**

通过该功能对数据进行采集通道配置，主要根据数据源要求、数据量大小、网络情况进行配置。

支持采集通道管理能力， 支持采集接口机管理能力，支持采集通道在采集接口机上的动态部署、卸载、启动和停止，支持常用采集协议，支持分布式热备，采集任务自动救援。

* + - 1. **采集任务管理**

通过该模块管理数据采集任务，可对采集任务进行创建、执行、关闭等操作，采集任务需关联采集通道。

采集任务支持精细化管理功能，采集任务具备管理采集数据源、采集方式、采集协议、采集周期等功能。

采集任务管理需包括采集任务的查询、新增、编辑、详情查看、启停和日志功能。通过前台页面配置的采集任务进行数据采集，记录采集数据的全量信息，并可查看采集日志信息。

* + 1. **数据质量控制**

系统接入多种来源的海量异构数据，这些数据的格式不统一，并且可能会存在数据输入错误、和数据不完整和数据重复等问题，系统支持对数据质量进行监控，并及时清洗对应脏数据，得到标准的、干净的、连续的数据，提供给数据统计、数据挖掘等使用。

* + 1. **数据处理**

数据处理包括数据格式转换、过滤/替换、数据富化、数据解析、数据归并、数据标签、数据校验、数据更新、数据脱敏、数据解密、数据加密、数据存储和数据管理等。提供不少于12种数据加工分析方式，通过对采集后的原始数据进行解密、解析、提取、过滤/清洗、转换、关联、标签、脱敏、排它等操作，实现对安全数据的统一加工，形成统一的数据存储结构，为后续数据建模，场景挖掘，提供数据基础；根据不同数据类型和访问频率、性能要求存入不同类型存储介质，支持不少于6种数据库，包括HDFS、Clickhouse、ElasticSearch、MySQL、Redis、Ka\*\*a。

* + - 1. **数据格式转换**

数据格式转换可以保证数据采集过程中遵循统一的存储格式规范，支持对各种类型数据的转换规则，避免乱码、时间格式不统一等情况。

* + - 1. **过滤/替换**

针对数据格式的不一致、数据输入错误、不完整或冗余等数据问题，支持以条件规则形式进行过滤或替换，减少各种脏数据。

安全事件数据过滤/替换功能包括但不限于：

* 数据过滤：将满足条件的数据进行过滤。可配置字段名、条件。当选择的字段名在选择的条件上满足时，过滤该条数据。
* 数据替换：将满足条件的字段值统一替换为指定值。可配置条件字段名、条件和替换值，以及要替换的字段名和替换值。
  + - 1. **数据富化**

采集到的原数据往往缺乏业务属性信息，因此需要丰富数据本身，通过关联补齐后形成完整的业务信息，以便于后期的统计分析。

支持对数据提供静态补全和动态补全的能力。

* + - 1. **数据解析**

将采集到的流量元数据、威胁告警数据、检测设备日志、级联上报数据等，根据不同的数据类型，分别对数据进行统一格式化处理，满足系统存储层数据格式定义的要求。标准化之后的数据保存原始日志，在符合相关法律法规的基础上，为网络安全事件的全流程溯源提供原始数据备查。

将采集到的流量元数据、威胁告警数据、检测设备日志、级联上报数据等，根据不同的数据类型，分别对数据进行统一格式化处理，满足系统存储层数据格式定义的要求。标准化之后的数据保存原始日志，在符合相关法律法规的基础上，为安全事件的全流程溯源提供原始数据备查。

* + - 1. **数据归并**

数据归并支持对采集的原始数据进行归并，如对同一事件的多次告警进行归并，对同一会话的日志进行归并等。

* + - 1. **数据标签**

数据处理过程支持通过打标签的方式对数据进行灵活分类。基于富化后的数据，结合数据所属业务系统、设备类型等信息，在原数据基础上进行标记。实现对数据的分类规整与管理，同时为基于标签的数据快速检索与安全分析模型奠定基础。

* + - 1. **数据校验**

从采集的数据中检测损坏或不准确的数据，是指识别数据的不完整、不正确、不准确或不相关部分。

为保证数据采集过程中遵循标准的协议格式规范，针对由于安全设备版本更新出现的数据格式变化等原因引发数据异常采集进行告警提示，及时减少由于数据采集异常导致的安全监测与预警能力下降的问题。

支持对数据字段格式和整体数据格式进行校验，格式校验包括但不限于：数据格式校验、IP地址校验、数值校验。

* + - 1. **数据更新**

提供数据更新服务，基于数据服务模块提供数据更新服务接口，通过图形化界面或接口直连的方式，对主数据进行更新操作。

* + - 1. **数据脱敏**

提供数据脱敏服务，对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。

不同密级用户间进行共享数据资源，需要对数据尤其是高密级数据进行必要的脱密处理。

* + - 1. **数据解密**

适用于敏感日志或基础数据采集后的解密，并将解密后的数据提供给后续节点进行数据处理。数据解密节点功能包括：解密范围配置、解密方式配置。

* 支持自定义解密范围需包括：全文解密、指定字段解密（可指定多字段）；
* 支持解密方式为：国密算法解密、base64、URL解码。
  + - 1. **数据加密**

数据加密服务，接口具有相应的安全保障机制，保证关键敏感数据在传输过程中的保密性、完整性和可用性。

数据库加密要求敏感数据以脱敏的形式存在，保证存储介质丢失和数据库文件被非法复制的情况下，数据的机密性。

在保证敏感数据安全的同时，最大程度的保证数据库的性能。

* + - 1. **数据存储**

数据存储需包括数据归档管理、存储方式配置、存储时间配置等。

1. 数据归档管理

将数据作为管理对象、以安全数据资产评估分析结果为导向统筹考虑数据的生命周期，达到对存储和计算资源的有效释放，提高资产利用率。

1. 存储方式配置

存储方式管理用于维护存储地址及配置，为资产定义提供存储相关数据支撑。

1. 存储时间配置

按照规定留存相关的网络日志不少于六个月，根据不同数据的保留周期，进行存储时间设置。

根据《中华人民共和国网络安全法》第二十一条第三项规定，“采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月”。

* + - 1. **数据管理**

数据管理包括索引管理、数据质量监控、数据策略、数据治理全过程管理和安全字典等。

1. 索引管理

对系统分析所得的标准化数据建立索引进行管理。

1. 数据质量监控

对数据处理过程中的数据质量进行集中监控与管理，保障数据处理过程中的准确性、完整性与及时性。

* 支持对于数据表级和字段级质量规则的定义，明确数据表、字段的质量要求；
* 内置表级和字段级规则模板，规则类型包括：及时性、波动性、重复数据、规范性、唯一性、空值、重复值；
* 支持通过内置模板方式和自定义SQL方式进行规则的创建；
* 规则配置支持阈值设定、绑定数据资产和进行规则试跑验证操作；
* 通过数据资产维度查看离线稽核和实时稽核规则数量和告警数量并支持告警结果的处理。

1. 数据策略

支持数据归档策略配置、数据共享策略的配置。

1. 数据治理全过程管理

提供数据治理全过程管理能力，帮助本系统对各个数据源、数据处理节点的数据情况的展示和运行分析，能够可视化的展示系统所有数据的流动情况，并能够展示针对异常的数据情况进行预警。

1. 安全字典

通过图形化数据管理界面，查看并控制安全数据字典的数据结构、数据内容。

* + 1. **数据共享**

数据共享包括数据共享服务管理、数据共享服务订阅和数据共享服务订阅等功能。

* + - 1. **数据共享服务管理**

数据共享服务管理的功能，需包括安全数据集市的展示、新增、修改、删除功能，安全数据资产的查询、编辑、删除、上架/下架、详情查看，订阅申请工单审批功能。

选择数据资产查询条件或重置查询条件，根据查询条件读取数据资产信息并展示，展示信息需包括资产分类、资产名称、资产编码、资产描述、存储方式、状态（上架、下架）。

* + - 1. **数据共享服务订阅**

数据共享服务订阅，主要提供界面化数据共享服务目录功能。

* + - 1. **数据共享服务使用**

数据共享服务使用包括实时场消费服务、安全日志检索服务、安全数据备份服务、安全数据集市共享服务和安全结构化数据服务等。

* 实时场景消费服务：为安全业务提供时消息队列，支持各类实时分析场景服务。
* 安全日志检索服务：为用户提供分布式、高扩展、高实时的数据检索引擎，提供海量数据中查询符合检索条件信息的能力。
* 安全数据备份服务：支持用户对存储在关系型数据库，全文检索引擎，数据仓库等的数据向分布式文件系统进行备份，用户可以自定义文件名称。存储于分布式的数据按照设置周期进行存储，超过存储周期设置即行删除。单次备份数据周期，单文件条数可设置。
* 安全数据集市共享服务：即安全数据共享API，提供基于关系型数据库&非关系型数据引擎的数据查询接口化输出。
* 安全结构化数据服务：即实时数据查询服务，向数据消费者提供可自定义查询SQL进行实时查询访问的能力。
  1. **接口管理**

接口管理包括数据接口管理、控制接口管理、业务接口管理、监管接口管理和级联管理等。

**3.4.1 数据接口管理**

数据接口管理包括数据接口编辑和接口标准。

**3.4.1.1 数据接口编辑**

提供数据接入接口的增加、删除、修改、启动、停止等管理能力。

**3.4.1.2 接口标准**

遵循RESTful原则：

客户端-服务器模式：将系统分成客户端和服务器两个部分，分别处理用户交互和后端资源管理。

无状态：服务器不保存关于客户端的任何信息，每次请求都包含足够的信息来处理该请求。

缓存：采用缓存机制来提高服务器性能和用户响应速度，减少网络带宽消耗。

统一接口：通过统一的接口定义，使得客户端和服务端能够独立演化，且客户端能够更好地理解和使用API。

按需代码：服务端只返回客户端需要的最小数据集合，减少带宽的消耗。

分层系统：将系统分为若干层，每一层只与相邻的层进行通信，降低复杂性。

**3.4.2 控制接口管理**

控制接口管理包括控制能力清单、控制能力转换、控制接口管理和插件实例管理。

* 控制能力转换需屏蔽底层数据能力的多样性，结合业务需求，设计支撑中台服务与驾驶舱服务的控制能力清单，并在后台与控制能力清单中的能力进行映射关联，确保各动作、传输的准确性；
* 控制接口管理需提供与相关安全设备的接口管理功能，根据业务需要开启、关闭相关安全设备的控制接口；
* 控制能力清单至少包含了对终端管理平台、安全设备、数据安全设备等的指令下发接口、任务调度接口，具有IP\DNS\URL封禁、隔离、查杀、扫描等能力。
* 控制实例管理管理对接的接口插件实例，至少包含插件自定义、插件测试、插件热加载功能等。1）支持自定义插件的初始化参数，类型来完成插架的初始化；2）系统支持针对插件的测试，能够验证参数配置；3）系统支持针对插件设置相关的自定义Python脚本完成插架的参数处理，指令下发，返回值处理；4）系统支持插件版本管理，能够查看回退插件的历史版本；5）支持插件的导入导出功能，热加载实时生效。

**3.4.3业务接口管理**

业务接口管理包括业务接口编辑，与浙政钉对接、工单系统对接、全流量分析平台、华为云平台和考核评分系统等对接。

业务接口管理包括业务接口编辑，与浙政钉对接、工单系统对接、全流量分析平台、华为云平台等对接；实现对业务接口的增加、删除、修改、启动、停止等管理能力。

**3.4.4监管接口管理**

为及时向监管部门反馈和处置各类网络安全事件通知，系统预留相应的接口，支持北向接口向其他平台提供数据外发和查询能力，发送通道包括UDP、FTP/SFTP、KA\*\*A等，支持对外发数据进行格式化转换（统一编码、映射转换等）以及数据组装方式设置（包括但不限于json、自定义模版、syslog等），并支持按需限制外发速率。

**3.4.5级联管理**

遵照《国家电子政务外网平台二期工程（中央投资部分）标准规范GWB 18-2019 运行支撑平台对接与实施规范》与省级平台进行运维数据对接。

**3.4.5.1 数据协同**

* 支持数据协同，支持将安全告警、安全事件、文件报表、漏洞及各类统计数据的自动上报。
* 将告警数据分为网络攻击告警、恶意程序告警、数据安全告警、其他告警等内容。
* 按照要求开发级联注册、级联监控、级联注册情况上报接口、告警数据上报接口等12类接口。
* 级联接口管理主要包含接口规划与设计、质量和性能监控、接口变更管理等信息。
* 数据上报主要上报告警数据、安全事件、漏洞信息、文件报表等。

**3.4.5.2 风险预警**

实时接收省级协同系统下发的预警信息和向省级反馈预警阅读状态等。

预警信息包含风险事件类型、风险事件级别、风险事件时间、风险事件位置、风险事件详细信息、风险事件处置建议等，支持预警的接收、跟踪、处置等全生命周期信息。

**3.4.5.3 事件协查**

支持事件协查工作流，在协查工单中实现对完整的协查流程的追踪，记录每个处理节点的处理时间、处理单位、处理人员、附件、描述等信息。

支持将预警信息跟本地日志的结合分析。

**3.4.6 其他系统数据接入**

本系统需采集绿盟、奇安信、安恒、华为、阿里等厂家的设备和平台类的日志。包含绿盟的网络安全协同管理平台、抗D设备ADS、IPS、WEB应用防火墙、漏扫等22个产品；包含奇安信的态势感知平台、威胁分析系统、堡垒机、终端管理平台等4款产品；包含安恒的态势感知平台、流量分析系统、WEB应用防火墙、安全审计、流量安全监控等8款产品，阿里和华为的云管平台、交换机、服务器、安全产品等；包含科来、天融信、F5、艾科、盈高、安华金和等8个厂家的全流量分析系统、数据库防火墙、数据脱敏系统、终端管理平台、流量审计系统、准入系统、负载均衡等产品和待招标的机房环境检测产品、数据安全产品等。

**3.4.7 接口清单**

**3.4.7.1 数据接口**

与安全设备、网络设备等所有相关设备的对接，采集网络安全相关的日志、运行日志、审计日志等。

**数据接口说明**

| **对接设备** | **内容** | **作用** |
| --- | --- | --- |
| 网络安全协同管理平台、态势感知平台、数据安全态势感知平台、阿里云华为云、科来业务性能管理系统、数据库管理平台等 | 与现网中的所有相关的设备做接口对接，采集网络访问、告警日志、恶意样本、认证授权、运行日志、网络质量、监控指标日志、审计日志、状态运行日志、流量日志、网络安全事件等数据，做所有日志做格式转换、替换、富化、解析、归并、标签等。 | 与安全设备、网络设备等所有相关设备的对接，采集网络安全相关日志、运行日志、审计日志等进行分析处理，形成数据资源池。 |

**3.4.7.2 控制接口**

提供与终端管理平台、安全设备、数据安全设备等软硬的控制接口开发。接口主要分成指令下发接口（平台与设备的指令下发通道）、任务调度接口（平台用于对设备任务进行排序和调度的）两大类。

**控制接口说明**

| **对接设备** | **内容** | **作用** |
| --- | --- | --- |
| 安全设备、数据安全设备等防护类设备 | 联动安全防护类的产品对恶意IP地址阻断等操作。 | 当内网中发现网络安全事件，需要联动防护设备做处置时，系统调动现网中的安全防护类产品的接口，并下发指令，联动处置。 |

**3.4.7.3 业务接口**

（1）与业务系统对接，如阿里云、华为云等业务系统等共享数据；采集IP地址库、工单信息、应用系统的运行状态等信息。

**业务接口说明**

| **对接设备** | **内容** | **作用** |
| --- | --- | --- |
| 网络安全协同管理平台、华为云、阿里云等 | 与业务系统(如阿里云、华为云等)实现数据共享，如应用系统的运行状态等信息。 | 实现系统的运行状态、资源使用情况等数据共享。 |

（2）按照浙数局发〔2023〕2号文件附件7，对部分数字化改革重大应用的日志进行采集和归集，采集字段包括用户标识、用户类型、地区编码、操作类型、操作标识、操作时间、操作时长、操作状态等。经过数据治理后，形成统一使用的JSON模式和统一的数据格式。归集数据包括但不限于用户标识、用户类型、地区编码、操作类型、操作标识、操作时间、操作时长、操作状态字段以统一格式推送至SLS日志服务。

**3.4.7.4 监管接口**

监管接口主要涉及与网络安全监管单位市网信、公安互联互通，网络安全事件上报及情报共享。

**监管接口说明**

| **对接设备** | **内容** | **作用** |
| --- | --- | --- |
| 市公安、市网信等平台 | 与监管部门的平台实现对接；对数据格式做转化，对监管部门发送的日志做标准化处理，能按着对方平台的要求，重新定义数据格式。 | 实现网络安全事件上报、情报等共享。 |

**3.4.7.5 级联接口**

遵照《国家电子政务外网平台二期工程（中央投资部分）标准规范GWB 18-2019 运行支撑平台对接与实施规范》与省级平台进行运维数据对接。

**级联接口说明**

| **接口功能** | **功能描述** |
| --- | --- |
| 省级平台 | 遵照《国家电子政务外网平台二期工程（中央投资部分）标准规范GWB18-2019运行支撑平台对接与实施规范》，开发对接12种类型的接口，上报告警数据、网络安全事件、漏洞信息等。 |

**3.4.7.6 区县级驾驶舱接口**

为满足10个区（县、市）以及2个功能园区的领导驾驶舱的11个大屏的数据需求，基于网络安全协同管理平台、抗D设备、IPS、防火墙等网络设备、安全设备等查询筛选设备接口，API接口包含Restful、websocket两类，对应数据库统计型数据和实时交互数据的推送，并支持基于用户角色权限，按设备类型、归属维度进行数据动态差异推送，保障安全性的同时，满足不同角色用户的数据使用需求。

**3.4.7.7 其他接口**

根据宁波政务信息化建设工作的规划，本系统将参照本建设方案内的有关内容与谋划建设的安全监管平台、安全设备等进行对接。

* 1. **第三方威胁情报对接**

随着网络攻击事件依旧层出不穷，在不断加强对网络安全、数据安全的保护力度的同时，力求更及时和准确地发现和处置潜在的网络威胁。为了打造主动安全防护、对恶意威胁追踪溯源、了解安全发展态势，本项目将采购两家威胁情报。

* 1. **基础设施层建设**

基础设施层设计包括数据安全监管建设、机房安全监管建设和安全防护软件和设备建设，依托宁波市政务云基础设施资源，采用信创云进行部署。通过采集云安全监管、网络安全监管、数据安全监管、终端安全监管、应用安全监管、机房安全监管等数源的监管数据，为系统奠定数字化底座。

* 1. **数据安全监管建设**

本项目数据安全监管建设是通过部署数据库监测系统和数据库权限系统软件实现。

* + 1. **数据库监测系统**

## 针对宁波市政务云的基础数据库和专业数据库及所部署的主机系统部署一套数据库统一监控平台，对数据进行实时监控预警、故障快速定位以及性能分析、SQL代码审核等功能，同时能够实现一键完成数据库健康报告。兼容Oracle、MySQL、达梦、人大金仓在内的11种主流数据库，同时也支持服务器基础监控，可以进行统一监控管理。支持通过API接口或者定制化方式推送相关数据。

|  |  |
| --- | --- |
| **指标项** | **指标内容** |
| 定制开发 | ▲为满足对跨网段多云环境数据库资源的统一监控，需支持通过API接口或者定制化方式推送相关监控数据 |
| 简易安装运维 | 支持全信创环境（国产架构CPU + 国产操作系统 + 国产数据库 + 国产中间件）安装部署；支持容器模式部署；支持双机高可用模式部署；支持一键自动化安装 |
| 采集组件可分离部署，支持对跨网段多云环境的数据库进行统一监控管理，无需多次部署产品 |
| 可通过页面来配置监控数据自动清理机制 |
| 授权配置 | 支持数量无限制的数据库实例 |
| 安全管理 | 支持HTTPS协议，确保数据传输的安全性；用户密码强度，期限可做配置 |
| 监控功能 | 无需在数据库服务器上安装任何形式的采集程序，也无需在数据库内部安装任何触发器或存储过程，避免给数据库带来未知的风险 |
| 能对多种关系型数据库Oracle、MySQL、达梦、人大金仓、SQL Server、PostgreSQL等，以及NoSQL数据库Redis、MongoDB进行实时监控、故障诊断、性能分析。可及时发现数据库的可用性和性能问题 |
| 提供慢SQL列表，支持通过下钻查看SQL文本，资源消耗，运行详情，并提供SQL优化建议 |
| 能够对每个数据库实例在不同时间区间的资源使用量进行精确测量，并能自动生成相关资源的时间图谱，可评估的系统资源包括每个数据库实例的CPU、IO吞吐及延迟等性能指标，以及关键的等待事件 |
| 支持根据实际需要来自定义监控指标，满足不同团队对于不同数据库在不同使用场景下的监控需求 |
| 支持查看每种数据库的表、索引、视图等基本对象 |
| 数据库基本信息监控齐全，包括数据库版本信息、基本参数、CPU、内存、表空间等 |
| 针对当前或历史某一阶段数据库的运行情况给出优化报告，供DBA优化进行参考 |
| ▲提供至少3种方式自动调节监控指标采集频率，最大幅度减少对被监控数据库的额外影响。   1. 可根据指定的时间段来设置不同的采集频率，时间过后，采集频率自动恢复 2. 可根据指标的采集耗时，自动调节采集频率 3. 可根据系统负载的不同，自动调节采集频率 |
| 支持对云主机的CPU/内存/网络/IO等关键性能指标进行实时监控 |
| 展示功能 | 提供可自定义配置的大屏功能，统一展示数据库运行状态、空间信息以及性能指标。 |
| 可以为不同类型的数据库配置不同的大屏展示页面。大屏支持Oracle/MySQL/达梦/人大金仓 /PostgreSQL/SQL Server等多种数据库的信息展示 |
| 告警功能 | 支持对主机文件系统，数据库表空间的预测，用户可以定义阈值 |
| 支持对不同数据库的告警指标进行个性化配置；支持告警静默，在正常停机维护或压测期间，可免受告警侵扰 |
| 支持多条件组合告警，比如当磁盘使用率和磁盘剩余空间同时满足预警条件时，才会发出告警 |
| 体检功能 | 支持对同类型数据库一键巡检，巡检规则包含参数配置、性能等。巡检报告包含不同维度得分雷达图。支持用户自定义添加巡检规则 |
| 能够手动或者定时自动生成数据库健康分析报告，提供包括配置、性能、管理等方面的分析结果 |
| 报表功能 | 支持同一数据库实例在不同时间段的同一性能指标对比分析；支持同种类数据库同一性能指标在相同时间段内的对比分析；支持应用负载路径展示，分析数据库负载来源 |

* + 1. **数据库权限系统**

|  |  |
| --- | --- |
| **指标项** | **指标内容** |
| 授权配置 | 支持无限制数据库实例。 |
| 数据库支持 | 支持ORACLE、SQL SERVER、DB2、MySQL、达梦等主流数据库、国产化数据库、大数据平台、云数据库。 |
| 身份准入 | 支持身份的多因素认证,系统根据多维身份管理策略，自动判别登录主体的合法性，如不符合设定的身份管理策略，登录失败。 |
| 支持识别真实应用及SQL管理工具的MD5值，防止假冒应用及假冒SQL管理工具违规访问数据库。 |
| 安全登陆 | 支持通过应用信息识别应用的是否为真实应用，进行应用防假冒，识别假冒应用访问数据库，进行拦截阻断。 |
| 支持数据库运维工具免密登陆功能，当数据库管理人员通过工具登陆运维数据库时，通过数据库账号与数字证书的绑定，数据库管理员在运维PC工具中无需输入数据库用户名密码即可登陆已授权访问的数据库，避免运维数据库用户和密码泄漏，保障账号安全。 |
| ▲支持拦截指定对象的高危操作行为（可自定义），支持数据库权限变更行为管控 |
| 支持通过应用指纹信息识别应用的是否为真实应用，进行应用防假冒，识别假冒应用访问数据库，进行拦截阻断。支持数据库授权管理控制，包括数据库角色权限管理、数据库对象权限管控、数据库系统权限管理. |
| 敏感数据脱敏 | 支持基于列的业务类型，设置脱敏策略，实现相同的业务类型同时设置脱敏策略。 |
| 支持运维侧脱敏，针对不同运维人员返回对应的预授权结果. |
| 误操作恢复 | ▲支持oracle、SQL server、mysql、DB2数据库的误删除恢复，当误删除敏感数据时，系统应及时记录操作信息，并提供一键恢复的功能 |
| 告警 | 支持以图形、列表等方式查看告警信息，以列表形式展现的告警信息应当包含告警时间、告警内容、告警等级、用户IP、数据库代理IP、事件等。  告警方式至少包括：邮件、页面、短信。 |

* 1. **机房安全监管建设（机房基础设施管理平台）**

机房基础设施管理平台建设内容包括管理平台软件、监控模块、机房资产管理模块、运维管理模块、能耗管理模块、网络线缆管理模块、综合数据分析大屏、公共功能模块、机房管理模块、人员定位管理模块、第三方系统接口模块、移动端管理、数据处理及录入等。

* + 1. **管理平台软件**

为数据机房提供整体运维服务管理的综合性管理平台,集动环、安防、巡检、运维、资产、容量分析和能耗分析于一体，统一数据分析、统一综合报表管理。

权限管理：由用户定义角色，给角色赋权限。由用户角色管理界面，由用户给使用用户赋角色。采用未操作时，自动退出。保护用户操作时忘记退出操作界面。权限管理涉及整个系统安全，关系重大。

登录验证：对数据进行加密传输。

* + 1. **监控模块**

实时监控模块可以对UPS、供配电设备、电池监测、极早期火灾探测系统、消防系统、安防系统中的门禁管理系统、视频监控系统、边界入侵报警系统及其它第三系统，整合各子系统告警数据，集中告警输出。包括实时监控报警模块、动环实时监控、安防实时监控和监控报表。

* + 1. **机房资产管理模块**

机房资产管理模块包括资产可视化搜索、场地基础设施可视化、温度云图管理子模块、IT基础设施可视化、资产台账管理、设备信息管理、资产盘点管理、资产供应商管理、资产上下架管理、资产容量管理（房间级）、资产容量管理（机柜级）、资产报表等功能。

* + 1. **运维管理模块**

通过运维管理模块用户可以方便地管理系统的各项资源和服务。同时，该模块还可以提供各种监控和报警功能，帮助用户及时发现和解决机房设备的各种问题。

运维管理模块通过场景化设计，将运维管理的各个环节串联起来形成闭环。其中包括工作台管理、工单管理、计划管理、值排班管理、访客管理和运维报表等功能。

* + 1. **能耗管理模块**

能耗管理模块包括能耗指标管理、能耗分析管理、能耗报表。数据中心能源管理主要作为整体机房能耗评估的重要依据，为实现机房内的能源管理、能源分配、能耗计算、能源节约的指标化。完善机房能源基础数据体系，建立一套科学完善的能源利用、监督、管理、评价体系。

* + 1. **网络线缆管理模块**

通过平台资产管理模块属性管理网络线缆，采用图型化技术提供直观展示网络配线物理连接关系，可以通过设备资产属性、配线架端口号查询网络用途、本地端及对端连接设备及设备网络端口。方便运维人员对机房进行后期管理和维护。

* + 1. **综合数据分析大屏**

通过平台综合分析将概览统计、关键监控指标、能耗指标、趋势分析、资产统计、报警统计、告警状况、监控状况、运维值班人员等相关信息进行大屏展示。

* + 1. **公共功能模块**

公共功能模块包括通知中心、可视全局搜索管理、签到签退、知识库管理、机房界面组态和报表中心等。

* + 1. **机房告警模块**

告警功能主要有，温度过高过低时进行报警提示、容量超过一定阀值时进行报警提示、UPS状态不正常时进行报警提示、空调状态不正常时进行报警提示、消防设备不正常时进行报警提示、其他联网设备状态不正常时都可以进行报警提示。

* + 1. **人员定位管理模块**

实现集中化机房内人员的实时定位、并提供一周内人员活动轨迹查询，可以限定人员活动区域，非许可用户进入未授权区域提供报警提示。包括人员的位置实时显示、报警提示、轨迹回放和地图引擎对接。

* + 1. **第三方系统接口模块**

包含动环系统、门禁系统、视频系统和防盗系统等第三方软件接口集成接入。

| **序号** | **系统名称** | **说明** |
| --- | --- | --- |
| 1 | 动环系统 | 集成、展示（实时数据）、告警，需开放标准接口例如SNMP（支持获取所有实时数据） |
| 2 | 门禁系统 | 集成、展示（门禁进出记录查询、门禁开关状态查看）、告警，需开放标准接口例如ODBC自定义接口 |
| 3 | 视频系统 | 集成、展示（实时视频画面查看、历史视频查看）、联动，需开放标准接口例如SDK |
| 4 | 防盗系统 | 集成、展示（工作状态）、告警，需开放标准接口例如SDK |

* + 1. **移动端管理**

包括移动端服务、监控管理模块、资产管理模块、运维管理模块、报警管理模块和移动管理PAD等建设内容。

2台移动管理PAD，配置需求：用于执行巡检、故障工单任务。CPU核心数：八核，屏幕尺寸：11英寸，内存容量：128GB，运行内存：8GB，支持4G、无线WIFI。

* + 1. **数据处理及录入**

包括二维码标签系统、工业级二维码打印机、设备网络连线和设备资产。

2台工业级二维码打印机，配置需求：热敏和热转印模式，300DPI，打印速度6IPS，打印宽度104MM。

* + 1. **其他配置**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **需求说明** | **数量** | **单位** |
| 1 | 管理终端（**投标时提供终端和显示器节能产品认证证书，未提供将作无效投标处理**） | 采用国产芯片架构，国产操作系统，内存≥8GB，硬盘≥256G，SSD /显卡：2G独显 ，配套LCD-24′显示器 | 2 | 台 |
| 2 | 管理终端操作系统 | 国产操作系统 | 2 | 套 |
| 3 | 温度感知系统 | 每台机柜正、背面安装温度采集器并统一采集并接入管理平台，为温度云图管理子模块生成温度模拟云图提供数据源。含840只温度传感器及采集主机和采集软件、并将采集数据接入到现有环控平台。 | 1 | 套 |
| 4 | UWB定位系统 | 室内人员定位系统智能硬件（含UWB基站、定位信标、定位工牌、POE交换机、室内网关等）。 | 1 | 套 |
| 5 | 安全防护系统 | 终端安全防护系统（单机版） | 2 | 套 |
| 6 | 文档处理软件 | OFD文档处理软件 | 2 | 套 |
| 7 | 办公软件 | 专业版国产办公软件（如WPS） | 2 | 套 |

* 1. **安全防护软件和设备建设**

为保证政务业务的顺利推进开展，同时保障政务外网的网络安全，根据安全防护要求部署四台防火墙，组成两组高可用性集群。

为加强政务外网上系统网络安全检测和验证，于政务外网部署一台Web应用安全检测系统。

综上，本项目安全防护软件和设备建设内容如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **内容** | **参数** | **数量** | **部署位置** |
| 1 | 防火墙 | 1.配置要求：国产芯片，国产操作系统,≥6个万兆光口,冗余电源，网络层吞吐量(双向)：IPv4≥50Gbps，IPv6≥50Gbps。应用层吞吐量（单向）：IPv4：≥20Gbps，IPv6：≥20Gbps。TCP新建连接速率： IPv4≥250万/秒，IPv6：≥250万/秒。 TCP并发连接数： IPv4≥2800万，IPv6：≥2800万，6个原厂万兆单模模块，3年原厂质保；  2. ▲支持手工链路聚合及LACP链路聚合，实现对聚合组内业务流量的负载分担；  3. ▲支持一体化安全策略配置，可以通过一条策略实现五元组、源MAC、源地区、目的地区、目的端口、域名、应用、服务、时间、长连接、并发会话等功能配置,简化用户管理；（提供截图证明）；  4.支持独立审计策略，支持审计白名单；（提供截图证明）；  5.支持针对地址、应用设置入侵防御白名单，支持攻击规则搜索以及自定义规则，自定义规则支持导入导出。 | 4台 | 政务外网外联接入区 |
| 2 | Web应用安全检测系统 | * + - 1. 配置要求：CPU≥国产芯片8核，内存≥32G内存，硬盘≥256G 6G R/S，最大吞吐量≥3000Mbps，3年规则库升级、软件更新，三年原厂质保。       2. 支持检测主流操作系统（Windows、Linux、Unix）、数据库、Web应用（SQLServer、Oracle、MySQL）、中间件、路由器、交换机等漏洞。       3. 支持域名信息自动收集，包括IP注册信息收集、子域名和目录暴破。       4. ▲支持多种弱密码口令协议的猜测与分析，包括AFP、RDP、FTP、SSH、TELNET、MSSQL、MYSQL、SSH、SNMP、Telnet、Postgresql、ORACLE、SMB、VNC、POSTGRES、POP3、Windows等服务。       5. 支持攻击载荷的生成，载荷攻击支持包含Windows、AIX、android、BSD、BSDi、Firefox、JAVA、linux、Mainframe、netware、nodeJS、PHP、Python、ruby、solaris、unix等，生成的攻击载荷同时具备一定程度的免杀能力。       6. 支持漏洞可利用性验证。       7. 支持黑客攻击链高仿真模拟，可实现后渗透演示。       8. 支持代理（Proxy）攻击，有效绕过防火墙拦截规则。       9. 支持智能页面爬虫功能，模拟人工鼠标点击爬取页面信息，有效绕过防火墙拦截规则支持多页面；       10. 支持业务逻辑漏洞检测，如越权、登录验证码绕过/回显、Cookie提权等；   11.▲支持业务逻辑越权漏洞检测，能够根据不同的账号权限判断业务系统是否存在越权漏洞（提供功能截图）；  12.支持渗透测试进程实时监控，包括以进度条、百分比、危险程度、漏洞信息的形式进行直观显示。  13.支持实时显示渗透测试进度以及阶段性测试结果，包括主机名、开放的端口号、操作系统、开启的服务、设备类型、网络跃点数、漏洞信息、危险等级等。  14. ▲主机类漏洞资源库不少于14万条，WEB应用漏洞资源库不少于7千条（提供功能截图）。 | 1台 | 政务外网核心骨干网 |

* 1. **国产信创软件采购**

根据项目建设和部署要求，需配套采购28套国产操作系统、11套国产应用中间件和7套国产数据库管理软件。

**八、技术要求**

* 1. **技术架构要求**

根据项目建设目标、宁波市政务信息化网络安全信息现状，要求采用主流大数据技术进行技术框架搭建，以应对海量数据采集、处理、分析计算以及对外共享业务需求，保障系统性能的同时，为后期项目扩展打好技术基础。

* 1. **应用服务要求**

要求以应用即服务思维，构建应用服务，对应用系统中涉及的身份认证、接口调用、数据上报、统计分析等业务应用提供统一的服务管理，包括负载均衡、限熔断流、运行监控及统一注册配置，便于后期业务及性能快速扩展。

* 1. **智能分析模型要求**

要求基于系统建设形成的网络安全数据资源池，通过对数据的分析和学习建立各种分析模型，并不断优化提高事件分析的准确，建设包括但不限于智能失陷主机分析、信息智能探测、暴力破解智能分析、账号明文传输检测、后门木马检测等智能分析模型，提升监测预警能力。

* 1. **自动化能力建设要求**

要求采用分布式计算框架，融合多种算子（安全检测场景模版）建立新的算子（模型），实现云、网、数、端、应用、机房等多方多维监测数据的融合建模，为多种安全场景提供智能化分析模型，通过对数据进行情境关联来丰富数据，建立资产、流量、告警、漏洞、行为等数据的关联关系，并借助高级统计技术、数据挖掘技术、行为分析技术、机器学习、人工智能等技术来实现智能分析。通过SOAR技术实现流程编排、安全剧本和自动调度的功能。借助安全编排技术将人员、流程编入剧本中，并支持动态调整。通过安全能力编排替换低级手动任务，实现对各个安全组件标准接口进行自动化调用，增加自动化和安全协调，缩短事件响应时间，同时提高准确性。

* 1. **系统集成要求**

1.省级系统集成要求

本项目系统要求对接省网络安全协调指挥平台，并支持与省级系统数据共享。

本项目建设周期内，中标单位需根据采购方需求，无条件完成本项目建设成果与上级要求的其他相关系统或平台的所有网络安全数据对接工作。

2.市内系统集成要求

本项目系统须与市内网络安全相关各类系统及设备进行数据对接，并与横向网络安全监管部门进行电子政务网络安全事件情报共享，并支持与各区（县、市）、各部门已有安全系统进行数据共享及数据整合。

* 1. **系统部署要求**

系统部署的总体要求是灵活、可扩展，根据招标方实际需求进行部署。

中标单位须对系统的可扩展性、高可用性等提供技术设计方案。同时针对可能出现的各类故障进行分析，并提供详尽的应急方案。

* 1. **信创需求▲**

**1、国产化要求：**一体化指挥系统、数据安全监管建设和机房安全监管建设需支持部署国产化环境，满足在宁波市信创云上运行，国产化服务器、操作系统、中间件等均以信创云支持为主；国产化服务器包括基于鲲鹏、海光等不同类型的；国产化数据库包括达梦数据库（DM）、南大通用baiGBASE数据库、OpenBASE、神州通用数据库等。国产化中间件包括金蝶、东方通、中创等中间件，满足在国产化中间件环境上的部署运行；国产化操作系统包括中标麒麟（NeoKylin）、银河麒麟、UOS（统信操作系统）等。

一体化运维指挥根据每日需处理6亿日志量，投标单位须在应标文件中对操作系统、数据库及中间件等系统软件配置进行详细的设计，以支撑本项目的应用系统的正常稳定运行。

**2、信创适配进度要求：**一体化指挥系统数据存储采用的大数据组件未采用国产技术，待本系统建设完成后，中标单位须根据国家、省市信创部署的相关要求，于2026年前完成大数据组件的信创适配等工作，将开源大数据组件替换为符合信创要求的大数据组件。

* 1. **网络信息安全保障建设要求**

本项目网络安全保障目标和对象为宁波市政务信息化网络数据安全一体化指挥系统所涉及的应用功能、应用支撑、数据资源体系等建设内容，主要涉及的用户为宁波市市县两级电子政务行业网络安全监管部门、市县两级业务部门和运营工作团队及人员等。参照网络安全等级保护2.0标准，**要求按照安全等级保护二级的要求进行建设。**

投标单位须对照《信息技术信息系统安全等级保护基本要求》、《信息技术信息系统安全等级保护测评要求》及《网络安全等级保护基本要求》进行网络安全风险分析，并做出针对性的网络安全设计，主要包括物理环境安全、通信网络安全、区域边界安全、计算环境安全、应用安全、数据安全、安全管理中心及安全管理机制等方面。

**九、性能要求**

1、系统用户及并发数。本项目要求支持用户数≥2000人，支持在线访问用户≥200人。

2、系统响应速度。系统具有良好的运行速度，有较高的数据承载能力，在网络稳定的环境下界面单一操作平均响应时间小于2秒，复杂操作平均响应时间小于5秒，在最大并发访问情况下，数据浏览单屏响应在2秒以内。复杂的大数据检索操作平均响应时间在10秒内。

3、系统可靠性。系统支持7×24小时不间断运行，系统可用率≥99.9%。

4、系统易用性。界面设计上应尽量友好，输出、输入方便，图表生成美观，检索、查询简单快捷，同时符合用户的业务操作习惯，最大限度的降低系统使用的复杂程度。

5、系统可扩展性。系统设计要充分考虑今后一段时期内的扩展需要。采用B/S三层架构的体系结构，系统必须是构件化、面向对象的，能够方便进行系统功能升级或者二次开发。

**十、****其他要求**

* 1. **开发方式要求▲**

本次系统开发采用驻场开发的方式，中标人须根据招标人要求的数量和质量配备现场开发人员，在招标人指定的工作场所开展各项开发和实施工作。项目不允许转包。

在开发依据方面，必须严格以招标方需求范围为准（包括业务需求、技术需求、需求规格说明书），如果有不同意见或建议，可以提交招标方考虑，但必须以招标方认可的需求为准。本招标书提供的招标需求为本次项目建设的基本需求，用于界定项目的建设及实施范围。投标单位须承诺在中标后根据招标需求进行深入的调研和分析，对项目建设内容进行进一步的细化设计后形成正式的需求规格说明书及设计说明书，并经招标人确认后作为项目开发、实施及验收的最终依据。

在系统正式验收前，因政策和制度等因素导致的需求变化，引起需要对软件进行修改、变更累计工作量在项目总工作量的33%以内，视为中标方应承担的项目风险，不视为新增工作量，招标方不再另外支付费用。

对招标书、投标书、合同、技术需求、业务需求、需求差异分析等各种文档中存在任何自相矛盾或表述不一致的地方，投标人应在投标前要求招标方澄清。如果投标人未在投标前要求招标方澄清，则在投标人中标之后，对这些不一致之处的理解，以招标方的解释为准。在沟通配合方面，中标方必须及时响应招标方要求，及时排查解决问题。

* 1. **项目管理组织**

**1.中标方项目管理要求**

1）在项目建设期间，投标人的项目团队成员未经甲方同意不可更换。

2）参与此项目的技术人员能够与用户进行良好的沟通，掌握相关领域的相关基础知识，具备相关应用和开发的能力。

3）投标人应列出详细实施方案，包括但不限于项目管理计划、项目进度计划、项目验收计划、项目组织结构（人员姓名、经验、学历和在本项目中的职责分工等）等。

4）投标人应在投标文件中提供详细的施工计划，应包括项目组织机构、项目实施流程、项目实施进度、项目实施安排。

5）中标后投标人所作的详细设计应完全满足用户的需求，同时不得与投标方案有实质性改变，除非招标人认可。

* 1. **开发、测试环境要求**

各阶段开发、测试所需的基本环境（包括工作环境、网络环境、系统软件、硬件设备等）由招标方指定。

* 1. **技术参数及其他说明**

1. 投标时必须如实提供投标产品的技术偏离表并加盖投标方公章。
2. 投标单位所提供的所有投标文件、技术文件及标准报价等相关资料必须真实、准确、合法，若经采购人查实有虚假、伪造行为，将提交财政监管部门处理。

3）在整个软件系统建设中，中标人如果使用第三方产品，必须作出采购人关于知识产权免责申明的承诺。

4）本项目软件开发需结合业务应用需求，有效利用宁波市大数据中心平台的信息资源进行开发；根据软件开发工具的使用需求，需在Linux环境下部署和管理部分应用和工具。

5）能够采取科学、合理手段保证项目在云计算环境实施过程中的数据安全、应用安全、可交互性与可移植性等云计算安全方面问题的解决。

**1.软件版本管理要求**

软件版本管理至少应满足以下要求：

（1）中标方应制定软件版本管理规范；

（2）中标方应建立软件版本控制制度，至少包括：系统升级时的版本管理、补丁管理；明确当前补丁是否包括前期的所有补丁，还是递增的补丁；统一项目的版本号等。如果系统升级影响到其他项目，应提前通知招标方协调其他项目进行相应调整；

（3）中标方应提供具体版本控制的措施和方案。

**2.主要交付成果物**

招标人将从软件系统的实际操作、项目过程控制文档、分析设计文档、分析设计模型，阅读源代码等方面入手对交付成果物进行审核。

要求中标供应商提交的成果包括并不局限于以下内容：

1. 需求规格说明书；
2. 概要设计说明书；
3. 详细设计说明书；
4. 数据库设计说明书；
5. 测试方案、测试用例、测试报告；
6. 可运行的系统；
7. 全部源代码（第三方软件除外）；
8. 软件系统使用的全部软件工具的列表；
9. 各种培训教材；
10. 部署材料清单；
11. 系统安装手册（包括开发过程环境设置）；
12. 系统维护手册；
13. 招标人认为需要的其他材料。
    1. **项目团队要求**

必须按照投标文件上的人员组成，组建至少20人以上现场开发、维护和实施团队，并指定一名专职的项目经理（本项目项目经理只能有一名，且其为项目投标时拟定的项目经理，须提供项目经理的相关资质证明材料），负责项目整体管理、项目协调和调度等工作。

除项目经理外，项目组须配备1名专职的技术负责人，负责项目总体技术架构设计、重大技术问题处置及研发团队的管理等技术工作。并按照项目实施的要求，配置相应的项目管理、系统设计、开发、测试、培训、质量保证等人员。

项目经理和技术核心专家必须始终驻场，进行开发工作的组织和协调。

1.在开发、试点和推广阶段，中标方实施人员数量、能力必须符合招标方的要求。

2.如果招标方认为中标方在宁波现场的团队成员的水平不足以胜任工作要求的，中标方必须及时更换人员。如果在招标方提出人员更换要求后，中标方符合条件的更换人员未在两周内到位的，视同违约，招标方可以无条件地按每人20万元的标准在合同价款中扣除。

3.中标方应保证项目队伍人员充足和人员结构合理，以便于项目顺利进行，并应任命一名专职技术负责人和专职项目经理。

技术负责人应具备以下条件：

1. 具有5年及以上IT项目开发工作经历；
2. 具有大型信息系统软件开发项目经理；
3. 具有优秀的计划、沟通、设计能力；
4. 熟悉电子政务信息化网络安全相关业务。

项目经理应具备以下条件：

（1）具有5年及以上IT项目管理工作经历；

（2）具有大型信息系统软件开发项目管理经历；

（3）具有优秀的计划、沟通和管理能力；

（4）熟悉电子政务信息化网络安全相关业务。

4.提交开发团队的成员名单及个人简历，并承诺在开发周期内的稳定，未经招标方同意，不得更换项目经理和技术核心专家。同时须说明应标人内部资源的协调和调动方式。项目组所有的人员必须遵守岗位职责和各项管理制度。

5.在项目参与人员（包括管理人员、开发人员等）方面，中标方务必确保相关人员的自身能力和工作态度等各个方面能满足项目的要求，对相关人员的选用和考评由招标方共同参与。

6.中标方要协助招标方培养系统运维技术力量，提交专门的培养计划和方案。除非不可抗力，保证核心技术人员的稳定，核心开发人员在系统推广应用完成之前，不能变动，整个项目人员的流失率不得超过30%。跟系统维护期内要求一致。

7.项目经理、技术负责人和其他成员在项目开工至初验完成均须常驻施工现场，出勤率均须达到85%及以上。

8.项目经理和技术负责人如确需更换，必须经过招标方的同意，且新更换的成员的各方面资历不能低于前任，同时更换项目经理或技术负责人须向招标方支付80万元/人的违约金（除不可抗力外）。

9.中标方若更换项目驻场开发、维护和实施团队成员(不包括项目经理和技术负责人)，必须经过招标方的同意，且新更换的成员的各方面资历不能低于前任。

10.项目驻场开发、维护和实施团队成员出勤率在85%以下的(按月考核)，项目经理和技术负责人根据未到天数，按照每人每天2000元支付违约金；项目驻场开发、维护和实施团队成员(不包括项目经理和技术负责人)根据未到天数，按照每人每天1000元支付违约金。

* 1. **质量控制要求**

1.项目质量要求

（1）中标方应接受招标方的有关软件质量情况的监督，无条件接受招标方的要求和建议，并进行认真整改；

（2）中标方应制定项目质量管理制度，明确项目质量管理工作流程及发现、解决质量问题的方法；

（3）中标方应根据质量目标层层分解，制定分层次的质量职责，并明确责任人；

（4）中标方应明确项目质量目标、质量标准，定期举办质量保障评审会和技术研讨会，提供评估流程以确保软件质量，明确项目产出物的评审，确定评审的方式和时间。

2软件质量要求

（1）中标方应制定软件质量测量计划、建立软件质量测量体系。

（2）应用架构设计、数据架构设计、基础设施架构设计、安全架构设计必须遵循信息化建设技术规范，满足招标方要求。

* 1. **测试要求**

软件测试是保证软件质量、提高软件可靠性的重要手段。为保证本项目的开发质量，中标方必须确保做好各阶段的软件测试工作。

1. **总体要求**

（1）本项目全面实施标准和规范化测试。中标方应完成全部业务功能、技术功能、安全功能和各种性能等各类测试的测试用例编写和实际数据采集工作。除非招标方同意，否则所有测试均以客观的测试用例和测试数据为准，不以个人主观判断作为测试标准。随着项目进度和各种变更，中标方应确保测试用例的更新；

（2）中标方应根据软件测试过程中的典型性问题、常见性问题和重要性问题建立软件测试知识库。

（3）如招标方委托第三方测试机构进行测试，中标方应予配合。

（4）中标方应提供测试所需工具，所提供测试工具应满足各测试项目的需要，招标方不对此额外付费。

（5）项目测试须按GB/T 15532-2008《计算机软件测试规范》和GB/T 9386-2008《计算机软件测试文档编制规范》进行软件检查、测试和文档的整理报送。中标方须保证对测试错误和缺陷进行及时修正、补充。

（6）为了提升交付效率以及避免人工测试可能造成的一些疏漏，中标方需要使用自动化测试技术，并且自动化测试覆盖率要满足一定的要求。

1. **测试准备**

本项目的测试准备工作具体包括但不限于以下内容：

（1）测试计划

中标方应提前制定测试计划，主要包括测试阶段划分、测试方法、工作流程、人员分工、进度安排等内容。测试计划须经招标方确认；

（2）测试组织

中标方应成立专门的测试组织，人员必须由高级测试经理和5名以上专业的、有经验的软件测试工程师组成，并对工作岗位和职责进行明确；

（3）测试方案

中标方应对每种类型的测试制定单独的测试方案，内容至少包括测试内容、测试环境、数据要求、测试范围与主要内容、测试工具与测试方法、完成准则等内容。测试方案须经招标方确认。

测试类型包括但不限于：

中标方实验室环境完成的单元测试、功能测试、性能测试、安全测试、集成测试、实验室压力测试等；

招标方测试环境完成的大规模压力测试、用户测试、系统测试等。

（4）测试用例

中标方应提供各类测试所需测试用例，至少应满足以下要求：

①测试用例的目标清楚，并能满足软件质量管理各个方面的要求；

②测试用例的组织和分类设计思路正确、层次清晰、结构合理；

③测试用例应覆盖所有测试点、所有路径和所有已知的用户使用场景；

④应有充分的负面测试用例，测试各种异常和例外情况。

⑤应根据测试阶段和情况的变化，及时更新维护测试用例。

（5）测试数据

中标方应准备模拟测试数据，数据必须满足测试需求，覆盖被测业务和测试边界，满足完整性、一致性等要求。

中标方应按招标方指定的范围，采集测试所需实际数据，并进行整理，满足测试需要。中标方必须对相关数据进行保密。

1. **中标方实验室环境测试**

中标方实验室环境的各种测试工作包括但不限于：

（1）单元和单元集成测试

①中标方应对单元测试流程进行规范，制订一定的覆盖率指标和质量目标，来指导单元测试设计和执行；

②中标方应严格按照单元测试流程进行测试；

③单元测试通过后，中标方应提交《实验室环境单元和单元集成测试报告》、单元测试用例及相关文档。

（2）功能测试

功能测试是对产品的各项功能进行验证，根据功能测试用例，逐项测试，检查本项目是否达到招标方要求的功能。

①中标方应对系统的各项功能进行验证，逐项测试，检查产品是否达到招标方要求的功能；

②中标方应严格按照功能测试流程进行测试；

③功能测试通过后，中标方应提交《实验室环境功能测试报告》、功能测试用例及相关文档。

（3）性能测试

性能测试是通过自动化的测试工具模拟多种正常、峰值以及异常负载条件来对系统的各项性能指标进行测试。

①中标方应选用合适的测试工具，测试软件在正常、峰值以及异常负载条件下的各项性能指标，性能指标应满足招标方需求；

②中标方应严格按照性能测试流程进行测试；

③性能测试通过后，中标方应提交《实验室环境性能测试报告》、性能测试用例及相关文档。

（4）安全测试

安全测试是检查软件安全防范能力。

①中标方应采用静态和动态检测工具，对软件进行全面检测，以发现软件在设计和编码中的错误、疏忽和其它缺陷；

②中标方应全面测试软件的安全功能；

③安全测试通过后，中标方应提交《实验室环境安全测试报告》、安全测试用例及相关文档。

（5）压力测试

压力测试是模拟工作负荷对软件进行破坏性测试和强度稳定性测试，测试软件在一定硬件环境下的性能指标。

①压力测试各类业务响应时间应当满足软件的性能要求；

②中标方应严格按照压力测试流程进行测试；

③压力测试结束后，中标方提交《实验室环境压力测试报告》、压力测试用例及相关文档。

1. **招标方测试环境测试**

实验室环境所有测试类型的《软件测试报告》经招标方确认，可进入招标方测试环境的测试。招标方测试环境所需设备由招标方提供，中标方负责安装部署。

中标方承担的工作包括但不限于以下内容：

（1）用户测试

①中标方应按招标方要求，准备测试方案、测试用例、测试数据。

②中标方应做好对用户测试结果的记录和问题的跟踪调试工作；

③中标方承担本测试阶段的所有费用；

④用户测试结束，中标方应提交《用户测试报告》、《用户测试反馈单》、测试用例及相关文档，由招标方确认。

（2）安全测试

安全测试是检查软件安全防范能力。

①中标方应采用静态和动态检测工具，对软件进行全面检测，以发现软件在设计和编码中的错误、疏忽和其它缺陷；

②中标方应全面测试软件的安全功能；

③安全测试通过后，中标方应提交《用户环境安全测试报告》、安全测试用例及相关文档，招标方确认。

（3）压力测试

在招标方测试环境下，中标方必须对本项目的各项性能指标进行大规模压力测试。

①中标方应制定压力测试方案，明确压力测试的测试环境、压力规模、加压时间等，压力测试方案必须经招标方确认；

②中标方应严格按照压力测试流程进行测试；；

③压力测试结束后，中标方提交《用户环境压力测试报告》、压力测试用例及相关文档，须经招标方确认。

（4）系统测试。

①中标方必须严格按照系统测试流程进行系统测试，并做好对测试结果的记录和问题的跟踪调试工作；

②系统测试的主要内容包括：健壮性测试、性能测试等；

③系统测试通过后，中标方提交《用户环境系统测试报告》、系统测试用例及相关文档，由招标方确认。

1. **主要交付成果物**

（1）测试方案和计划：应当包括各阶段各种测试类型的测试方案和计划。

（2）测试说明：应当包括测试标准和规范说明、测试设计说明、测试用例说明和测试规程说明。

（3）测试报告：应当包括各测试阶段和测试类型的测试报告。交付成果物应当满足科学性、完整性和准确性的要求。

（4）完成准则：中标方提供的所有测试类型的测试均已通过，并且《软件测试报告》和相关文档经招标方确认，视为软件测试完成。

* 1. **系统维护期要求**

自业主对本项目验收合格之日起，中标人须提供并现场派驻不少于2名由招标方认可的技术人员，负责一年内的数据治理和运行维护（包括软件升级、错误及维护性修改等，维护人员须常驻宁波，费用计入总价）。

在开发和维护期间的中标方人员变化必须经过招标方本项目的负责人同意。在服务期中一般不允许进行人员更换，如因特殊原因确实需要进行维护人员变换的，需提前通知招标方并指定新更换的人员，在征得招标方认可同意后，才能进行人员更换。在项目执行过程中，如招标方认为项目小组中工程师未具备维护的基本能力或不遵守招标方相应工作规定的，有权要求维护公司进行人员变换。

2.中标方必须提供详细的技术支持和服务方案。

* 1. **所有权声明**

1.招标方对项目实施过程中所产生的所有成果（包括发明、发现、可运行系统、源代码及相关技术资料、文档等）享有所有权（永久使用权、复制权和修改权等）。除本项目工作所需外，未经招标方书面同意，中标方不得擅自使用、复制招标方的商标、标志、数据信息、文档及其他资料。

2.中标方应保证在本项目中所有预装和为本项目安装的软件为在中国境内具有合法版权或使用权的正版软件且无质量瑕疵。

3.中标方应保证其所提供的产品及服务不侵犯第三方的知识产权，否则，由此给招标方造成的一切损失由中标方承担。

**十一、上线运行和培训要求**

* 1. **上线运行要求**

本项目的上线运行是指完成软件测试后，移植到生产环境下的运行。

1.中标方应完成运行前的环境准备工作，制定《上线运行工作总体实施方案》。

2.中标方应按照招标方确定的上线单位的范围和规模以及工作量大小，充分准备各类资源（人员、设备、用户手册、系统维护手册等），并进行合理配置，能够满足招标方上线工作的要求。

3.中标方应承担项目包含系统的安装部署、系统联调、和其他相关系统接口联调和日常技术支持等工作。

4.中标方应负责收集软件运行过程中发现的问题和用户的二次需求，修改完善应用软件功能，优化系统性能。

5.中标方应承担发现问题、提交问题、修改问题的责任，按照招标统一的问题处理流程执行，问题处理清单须经招标方确认。

6.中标方开发的软件存在缺陷或中标方配合不到位等原因，导致试运行工作失败或延期，责任由中标方承担。

* 1. **培训要求**

1.本项目的培训，是指中标方对招标方要求的使用和维护该软件的人员进行培训。

中标供应商有义务无偿培训招标方的技术人员，实现招标方的自我支持能力以及源代码级的自我维护能力。

2.培训由中标方负责师资及教材，由招标方提供场地和培训设备并负责组织实施。中标方必须派出用户认可的具有相关专业资格和实际工作经验的教师及辅导人员进行培训，主要培训教员至少应具有三年的同等内容的教学经验。

3.费用计入总报价。

**十二、验收要求**

项目的验收包括初验和终验：

1.初验

软件开发实施部署完成并经测试通过后，系统完成初验进入试运行，试运行时间为3个月。

2.终验

系统通过试运行后，中标方向甲方提出终验申请，甲方组织相关单位进行系统的终验。系统终验通过，进入正式运行阶段。系统终验收合格的条件必须至少满足以下三个要求：已提供了合同要求的全部设备、资料；试运行时性能满足合同要求；测试和试运行时出现的问题已被解决。

**十三、售后要求**

1.中标单位保证对软件系统提供3年的质量保证期，对硬件系统提供3年原厂质保和规则库升级服务。中标单位驻点人员不少2人一年。

2.质保期内因系统本身缺陷造成各种故障，软件系统应由中标单位免费提供技术服务和维修，硬件系统由原厂工程师技术服务及维修，费用由中标单位承担。

3.质量保证期自项目正式验收合格之日开始计算，质量保证期内，在接到系统故障通知后，投标人必须在15分钟内响应。对于影响系统正常运行的严重故障，投标人工程师及其它相关技术人员必须在接到故障通知后1小时内赶到现场，查找原因，提出解决方案，并工作直至故障修妥完全恢复正常服务为止，一般要求保证系统在4小时之内修复，并需要提供确保承诺实现的措施。

4.为保证系统正常、安全地运行，技术支持力量和优良的服务是系统正常、安全运行的保障。投标人应据此制定系统详细的技术支持与服务方案，包括服务内容、服务方式、服务响应时间、应急措施及组织结构等。

5.投标人须做出无推诿承诺。即投标人应提供特殊措施，无论由于哪一方产生的问题而使系统发生不正常情况时，并在得到采购人通知后，立即派工程师到场，使系统尽快恢复正常。

6.在质量保证期结束前，须由中标单位工程师和采购人代表进行一次全面检查，任何缺陷必须由中标单位负责修改。在修改之后，中标单位应将缺陷原因、修改内容、完成修改及恢复正常的时间和日期等报告给采购人。

7.中标人应提供电话免费咨询服务。

8.中标单位应确保本系统中所使用到的第三方软件应具备正版授权。本系统开发完成后，本系统的版权归采购人所有。

**十四、资金支付**

合同签订之日起7个工作日内采购方向中标供应商支付合同总价的30%作为预付款，项目通过初验后10个工作日内采购方向中标供应商支付合同总价的20%，项目通过终验后10个工作日内支付合同总价的50%。

**评标标准与评标办法**

一、评标原则

1、公平、公正地对待所有合格的投标人。

2、遵守《中华人民共和国政府采购法》等有关法律法规的规定。

3、评标必须以招标文件中各项规定条件为准。

二、**无效标**

资格审查由采购人负责，符合性审查及评审由评审委员会负责。凡出现以下情况之一的投标文件将被视为无效标，不进入技术评议及综合打分：

* 1. 符合下列条件之一的，资格性审查不合格：

（1）不符合政府采购法第22条规定；

（2）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记录名单在禁止参加采购期限的供应商（以投标截止日“www.creditchina.gov.cn、www.ccgp.gov.cn”网站查询数据为准，打印不合格投标人的查询记录网页一并作为资格审查资料存档）；

（3）不符合特定资格条件的（若有）；

（4）不符合政府采购政策要求的（若有）。

* 1. 符合下列条件之一的，符合性审查不合格：

**（1）未按要求提供诚信投标承诺书、投标函、开标一览表的；**

**（2）应当提供法定代表人授权书而未提供的；**

**（3）实质性条款不满足的；**

**（4）人员数量不满足招标要求；**

**（5）投标有效期少于招标文件要求的；**

**（6）投标人应填写全称，加盖与全称相一致的公章（不得加盖带有“专用章”等字样的印章），未按规定签署、盖章的，影响投标效力的；**

**（7）投标文件未按要求编制，内容缺失、不完整，导致无法评审的；**

**（8）投标价格错误且不同意按招标文件要求进行修正的；**

**（9）投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，应当要求其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；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。**

**（10）出现招标文件规定作无效标处理的其他情形。**

* 1. 法律、法规和规章规定的其他情形。

三、**废标**

凡出现以下情况之一的，本项目废标：

（1）合格投标人不足三家的；

（2）法律法规规定的其他情形。

四、评审程序

1、招标人工作人员按评审委员会名单核对评委身份，组织评委及监管等人员签到。

2、招标人工作人员宣布评审纪律，征询评委有无回避情形；

3、评审委员会确定评审组长，负责组织主持评审活动；

4、招标人工作人员对每个评委评审情况进行复核，有差错的、或畸高畸低的，提醒评委进行修正，评委拒绝修正的，提交评委会按少数服从多数原则集体决定，并记入评审记录内。情节严重的，报监管部门处理。

5、招标人工作人员协助做好价格分和评审情况的计算、汇总工作。

6、评审委员会形成评标报告，应由全体成员签字确认。有保留意见的可以在评标报告中申明，未申明且拒绝签字的视同默认评标报告并载明此情形。

7、招标人工作人员宣布会议结束。

五、评标方法

本次招标的评标采用综合评分法。

综合评分法：根据本项目招标文件的要求，按照本办法规定的内容和分值设置，对投标人的投标文件中进行评分，最终得出该投标的总分（保留2位小数）；按得分自高向低次序排出评标结果排序。

六、评标细则

首先根据招标文件的完整性、有效性及资格等方面进行审查，通过审查的投标文件才能进入综合比较与评议。

(一) 评分标准

评分表

|  |  |  |
| --- | --- | --- |
| 评分内容 | 分值 | 评审因素及说明 |
| 价格部分 | 15分 | 1. 投标货物为小微企业生产且使用该小微企业商号（商标）且投标服务由小微企业承接，该投标价格给予10%的价格扣除后参与评审（监狱企业和残疾人福利性单位视同小微企业）   2、投标人为大中型企业，接受分包的供应商为小微企业且分包金额不低于合同总金额的30%，给予4%的价格扣除后参与评审。  3、基准价为所有有效评审价格中的最低报价。  4、投标报价得分=基准价/评审价格×15（保留二位小数）。 |
| 资信商务及技术部分 | | |
| 技术 | 51.5分 | 技术参数符合度（10分）：根据投标人对招标文件技术要求的响应进行评议，任何一条未带“▲”招标要求的未响应或不满足的，每条扣0.2分；任何一条带“▲”招标要求的未响应或不满足的，每条扣0.5分，本项满分10分，扣到0分作无效标处理。（最小评审项“一条”说明：软件部分以三级标题为准，硬件部分有序号的以最下层序号为准，其它以自然段为准） |
| 项目需求的理解（16分）  （1）项目理解（4分）：根据投标人对项目背景、宁波电子政务外网的理解、网络基础和区域安全分析等进行综合评价。  投标人对项目理解分析比较深刻、全面、有针对性得3.1-4分；  分析基本合理、简单的得1.1-3分；  分析粗浅，缺少针对性的得0.1-1分；  未提及此项不得分。  （2）项目用途分析（4分）：根据投标人对项目的定位、目标、数据源类型等阐述的详细、全面、准确等进行综合评定。  针对项目用途分析的阐述详实程度全面、准确高等情况得3.1-4分；  针对项目用途分析的阐述详实程度较全面、准确度较符合得1.1-3分；  针对项目用途分析的阐述详实程度较简单、准确度基本符合得0.1-1分；  未提及此项不得分。  （3）重难点分析（4分）：根据投标人对项目建设工作的重难点作分级分析，是否层级清晰、分析深刻透彻，是否符合实际进行打分。  分析详细到位，层级清晰、分析深刻透彻，符合实际的得3.1-4分；  分析基本满足，层级逻辑基本可行，基本符合实际的得1.1-3分  分析内容简单，层级不够清晰，缺乏深度，基本符合实际的得0.1-1分；  未提及此项不得分。  （4）重难点解决方案（4分）：根据投标人对项目建设工作存在的重点难点问题的解决措施进行打分。  对本项目的重点、难点分析准确，且建议、措施较为合理、针对性强、切实可行，得3.1-4分；  对本项目的重点、难点分析较为准确，且建议、措施有一定的针对性和可行性，得1.1-3分；  对本项目的重点、难点分析一般，且建议措施的针对性一般，得0.1-1分；  未提及此项不得分。 |
| 业务应用层设计（4分）：根据投标人提供的应用支撑层设计与建设要求的完整程度、详细程度、与招标内容的贴合度、可行性等方面进行评价。  对业务应用层包含的领导驾驶舱、业务驾驶舱、运营工作台等模块功能设计理解清晰准确，完全符合招标要求，且技术方案有详实描述，并且落地可行性强，得3.1-4分；  对业务应用层包含的领导驾驶舱、业务驾驶舱、运营工作台等模块功能设计基本完整，对招标要求的各功能描述一般，且落地性一般，得1.1-3分；  对业务应用层包含的领导驾驶舱、业务驾驶舱、运营工作台等模块功能设计理解模糊，对招标要求的实现描述不够完整，落地性差，得0.1-1分。  未提供的不得分。 |
| 应用支撑层设计（4分）：根据投标人提供的应用支撑层设计与建设要求的完整程度、详细程度、与招标内容的贴合度、可行性等方面进行评价。  对业务支撑层包含的通用组件、系统引擎等模块功能设计理解清晰准确，完全招标要求，且技术方案描述完整、详实，并且落地可行性强，得3.1-4分；  对业务支撑层包含的通用组件、系统引擎等模块功能设计理解基本完整，基本符合招标要求，且投标描述一般，落地可行性一般，得1.1-3分；  对业务支撑层包含的通用组件、系统引擎等模块功能设计理解模糊，技术方案部分符合招标要求，技术方案描述不够完整，落地可行性差，得0.1-1分。  未提供的不得分。 |
| 数据资源层设计（4分）：根据投标人提供的应用支撑层设计与建设要求的完整程度、详细程度、与招标内容的贴合度、可行性等方面进行评价。  对数据资源层包含的分析引擎、数据库、数据治理、接口管理、第三方威胁情报对接的模块功能设计理解清晰准确，完全符合招标内容要求，且技术方案描述完整、详，并且落地可行性强，得3.1-4分；  对分析引擎、数据库、数据治理、接口管理、第三方威胁情报对接的模块功能设计理解基本完整，技术方案符合招标要求，技术方案描述一般，落地可行性设计一般，得1.1-3分；  对数据资源层包含的分析引擎、数据库、数据治理、接口管理、第三方威胁情报对接模块功能设计理解模糊，技术方案仅符合部分招标要求，技术方案描述不够完整，落地可行性不足，得0.1-1分。  未提供的不得分。 |
| 基础设施层设计（3分）：根据投标人提供的机房安全监管与建设要求的完整程度、详细程度、可行性等方面进行评价。  对机房安全监管的模块功能设计理解清晰准确，完全符合招标内容要求，且技术方案描述完整、详细，并且落地可行性强，得2.1-3分；  对机房安全监管的模块功能设计理解基本完整，技术方案符合招标要求，技术方案描述一般，落地可行性设计一般，得1.1-2分；  对机房安全监管的模块功能设计理解模糊，技术方案仅符合部分招标要求，技术方案描述不够完整，落地可行性不足，得0.1-1分。  未提供的不得分。 |
| 质量管控（4分）：根据投标人对项目建设工作中的针对本次项目过程的管理规范、风险应对、对不合格率识别与处置进行打分。  对系统研发从计划到交付的全流程管理健全、职责分明；具有完备的风险应对机制及措施；具备完善的不合格工作交付识别和控制能力，能有效防止其非预期的使用或交付，得2.1-4分；  投标人对系统研发从计划到交付的全流程管理不严密、职责和本次交付团队人员未一一对应；制定风险应对机制及措施，但有关机制与措施管理粗犷，管控效果一般，得0.1-2分；  未提及此项不得分。 |
| 合理化建议（2.5分）：根据投标人依据本项目服务要求、实际作业需求，针对项目建设要求、进度要求、技术要求、性能要求、售后要求等方面提出的合理化建议，建议是否具有可实现性、对本项目的开展是否有所帮助等情况进行打分。  建议合理，可实现性强，具有改进意义的得1.1-2.5分；  建议可实现性较差，几乎没有改进意义的得0.1-1分；  未提及此项不得分。 |
| 整体方案内容（4分）：评价技术方案的系统架构设计、资源分配、部署设计、安全设计、接口对接设计等内容的完整性、合理性和规范性。  整体方案描述全面、合理、规范，得3.1-4分；  方案设计基本服符合要求，设计不够细致的，得1.1-3分；  方案差的，得0.1-1分。 |
| 服务能力 | 21分 | 售后服务方案（5分）：  售后服务方案科学、合理、规范，响应及时，措施的可操作性强的得3.6-5分；  售后服务方案的科学性、合理性、规范性、响应的及时性、措施的可操作性较强的得2.1-3.5分；  售后服务方案的科学性、合理性、规范性、响应的及时性、措施的可操作性一般的得0.1-2分；  未提及此内容不得分。 |
| 投标人项目组人员配置（16分）：本项目是大型软件开发项目，项目人员需至少配置20人，项目经理、技术负责人及所有人员均需驻场本地开发，在服务期内需提供两名驻场数据治理专家。项目组人员不足20人将被视为投标无效。项目组人员（至少20人）均需出具所缴纳的社保证明（由社保部门出具并盖章的社保证明为准）。  本项目应分别配置1名专职项目经理和1名专职技术负责人。 （1）项目经理（5分）：  1）资质证书（3分）：具备有效①全国计算机与软件专业技术资格证书信息的系统信息项目管理师（高级）②全国计算机与软件专业技术资格证书信息的网络工程师证书③中国信息安全测评中心认证的注册信息安全专业人员CISP每满足一项得1分，提供证书扫描件，未提供的不得分。  2）项目经验（2分）：提供项目经理具备项目管理经验的案例，每个得1分，最高得2分。  注：项目经理需具备5年及以上项目管理经验（以信息系统项目管理师（高项）获取时间为起点），不满足则不得分；项目经理项目经验不限就职单位，需提供佐证材料，不提供的不得分。  （2）技术负责人（5分）：具备有效①中国信息安全测评中心认证的大数据安全分析师CISP- BDSA②中国信息安全测评中心认证的注册信息安全管理人员CISP-CISO③网络安全应急响应技术工程师CCRC-CSERE④数据安全能力成熟度模型测评师DSMM⑤中国信息安全测评中心认证的注册数据安全治理专业人员资质认证CISP-DSG，每满足一项得1分，提供证书扫描件，未提供的不得分。  （3）项目成员（3分）：项目团队人员证书要求①2个中国信息安全测评中心认证的注册信息安全专业人员CISP②1个国家重要信息系统保护人员CIIP-A③1个大数据安全分析师CISP-BDSA，每满足一项得1分，提供证书扫描件，未提供的不得分。  （4）数据治理专家（3分）：  服务期内需提供两名本地驻场数据治理人员。具备有效①全国计算机与软件专业技术资格证书信息的软件设计师②全国计算机与软件专业技术资格证书信息的信息安全工程师③中国信息安全测评中心认证的注册信息安全专业人员CISP。两人中任意一人满足一项得1分，提供证书扫描件，未提供的不得分。 |
| 商务 | 3分 | 投标人具有有效质量管理体系认证证书、信息技术服务管理体系认证证书、信息安全管理体系认证证书情况（3分）：每满足一项得1分，提供证书扫描件，未提供的不得分。 |
| 类似项目业绩 | 1.5分 | 投标人自2020年1月1日（以合同签订时间为准）至今具有类似项目实施案例的，每个得0.5分，最高得1.5分。提供合同扫描件。 |
| 讲标 | 8分 | 投标人结合招标要求对方案进行述标（支持现场述标或提供视频述标，述标以投标文件解密先后顺序进行），总体时长不超15分钟，述标内容包含对项目概况分析及实施规划、投标人能力展示）（8分）：  1.项目概况分析及实施规划的内容包含但不仅限于现状分析、网络拓扑分析、资源需求、设计思路、开发计划、安全保障措施等（3分）。  述标思路及逻辑清晰，述标内容贴合实际、详细、可行性强，得2.1-3分；  述标思路及逻辑比较清晰，叙述内容较符合实际、可行性较强，得1.1-2分；  述标思路不清晰，叙述内容一般，可行性差，得0.1-1分。  2.投标人能力展示包含数据源的接入、数据处理、数据质量及数据共享能力等，综合评定（5分）。  对数据采集通道的可视化管理能力，如：采集机和采集器的管理等(0.1-0.5分)。  对支持的数据协议采集能力，如：JDBC、SNMP、Syslog、ka\*\*a、http、netflow、plusar、webservice、RabbitMQ等(0.1-1分)。  对数据处理能力，如：格式转换、过滤、替换、关联补齐、数据解析、数据标签、数据校验、脱敏、解密等（0.1-1.5分）。  数据质量管理能力，如：数据质量稽查任务管理（数据质量的完整性、唯一性、波动性、准确性、有效性、结构性、及时性等）、异常资产统计、告警任务状态管理等（0.1-1分）。  数据共享能力：共享服务管理、安全实时场景消费、日志检索、数据集市共享、数据备份等能力进行综合评定（0.1-1分）。 |
| 合计 | 100分 |  |

由评委对各投标人的投标文件进行审阅，然后根据需要对投标人进行询标和评议，并按以上指标（除价格部分外）进行记名打分。

统计、汇总所有评委对每一份投标文件的评分，然后用算术平均法求出每一份投标文件非价格部分的平均得分。

1. **价格部分**

先由评委会对各投标人的分项报价进行分析。审查投标报价是否符合招标文件的基本要求，有无明显开口、漏项、漏量等情况，在取得基本一致的意见后进行判别计算。对出现漏项、漏量情况的标书由评委会进行调整，得出评估价。

1. **其他部分**

除明确给出评判标准的项目外，由评委根据投标人情况综合评定，各项指标的最小打分单位为0.1分。

1. **最终得分与中标人的确定**
2. 各投标人最终分按以下方法进行计算：最终得分＝价格得分+其他得分；
3. 各投标人的最终得分若出现并列分，则由报价低的排列在前，报价也相同的则由技术得分高的排列在前，价格和技术得分均相同的则由随机抽取的方式确定。

评审委员会在审标、询标的基础上根据事先制定的评标办法对各投标人的投标文件进行评定，评出最高得分的投标人为推荐中标人。推荐中标人公示无异议的将被确定为中标人；**推荐中标人的投标文件若存在以不真实材料来谋取评审优势的，将失去中标资格，由得分次高的投标人为推荐中标人进行公示，以次类推（需重新招标的除外）**。确定中标人后由招标人向中标人发出中标通知书。

**第三部分 投标人须知资料表**

|  |  |  |
| --- | --- | --- |
| **序号** | **内 容** | **说明与要求** |
| 1 | 招标人情况 | 招标人名称：宁波市政府采购中心  质疑接收：吴先生 TEL：0574-87187956 FAX：87187961  地址：宁波市鄞州区宁穿路1901号市政务服务中心五楼  邮编：315066 |
| 2 | 采购方式 | 公开招标 |
| 3 | 联合体投标 | 🗹不接受；🞎接受，最多 家，联合体要求：XXX。 |
| 4 | 专门面向中小企业招标 | 🞎是；🗹否。 |
| 5 | 分包 | 🗹同意，投标人为大型企业的，分包意向承诺中中小企业合同金额应不低于合同总金额的10%。**本项目允许分包的建设内容为数据库监控系统和机房安全监管建设（机房基础设施管理平台）**。  🞎不同意分包。 |
| 6 | **集中现场踏勘(答疑)** | 🗹无；🞎有。 |
| 7 | 讲标与演示 | 🞎无；🗹有，具体要求见需求说明。 |
| 8 | 备选报价方案 | 🗹不接受；  🞎接受，投标文件未明确主备方案的视为无效标。 |
| 9 | 服务对象及地点 | 采购人指定，详见项目需求说明。 |
| 10 | 投标有效期 | **开标后90天** |
| 11 | **招标文件工本费及中标服务费** | 不收取 |
| 12 | 投标保证金 | 不收取 |
| 13 | 履约保证金 | 🗹不收取；  🞎收取，合同金额的1%，合同签订时向采购人提交履约保证金（履约保证金应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交），合同履行完毕退还,但不计利息。 |
| 14 | 采购资金支付方式、时间和条件 | 🞎一次性支付：验收合格后15日内一次性支付合同金额的100%；  🗹分批支付：详见项目需求说明。 |
| 15 | 投标文件提交方式 | **本项目通过政采云平台进行电子投标，投标人须通过浙江政府采购网（zfcg.czt.zj.gov.cn）发布的政采云电子交易客户端（浙江政府采购网首页“下载专区”下载）制作并上传加密电子投标文件。** |
| 16 | 其他 | **无** |

**第四部分 投标人须知**

**A 总则**

1、适用范围

1.1本招标文件适用于投标邀请中所述项目的采购。

2、定义

2.1“采购人”系指依法进行政府采购的国家机关、事业单位、团体组织。

2.2“集中采购机构”即宁波市政府采购中心，系指统一组织实施纳入政府采购目录项目采购活动的非营利事业法人。

2.3“招标人”系指组织本次招标活动的集中采购机构。

2.4“投标人”系指参加本次招标活动符合资格条件的供应商。

2.5“投标人代理人”系指参加本次投标活动的投标人授权代表。

3、合格的投标人和投标产品

3.1合格的投标人应具备以下条件：

3.1.1符合《政府采购法》第二十二条第一款规定的关于供应商基本资格条件。

3.1.2投标人应遵守中国的有关法律、法规和规章。

3.1.3有能力提供本次招标产品并符合投标邀请中规定资质要求的合法营销资格的国内企事业单位，均可参加投标。

3.1.4投标人与采购人一般应无任何直接或间接的关联。**有关联的，投标人应当在投标截止时间3日前告知招标人，在“诚信投标承诺书”中如实说明，并提供关联关系材料。**

3.1.5投标人存在下列关联关系情形之一的，不得参加同一标包投标：

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

**（2）为项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该项目的其他采购（具体实施）活动。**

3.1.6一个投标人对一个标包只能提交一个投标文件。

3.1.7投标人代理人只能接受一个投标人委托参加投标。

3.1.8如投标人代理人不是法定代表人，须持有《法定代表人授权书》。

3.1.9除招标文件有规定外，两个或两个以上供应商可以组成一个投标联合体，以一个投标人的身份参加投标。

以联合体形式参加投标的，联合体各方均应符合《政府采购法》第二十二条第一款规定的关于供应商基本资格条件，联合体中至少应当有一方符合招标文件规定的特定条件。

联合体各方之间应当签订共同投标协议，明确约定联合体各方承担的工作和相应责任，并将共同投标协议连同投标文件一并提交。

联合体各方不得再以自己名义单独在同一项目中投标，也不得组成新的联合体参加同一项目投标。

3.2合格的投标产品或服务

3.2.1应该是中国境内生产的产品或提供的服务。

若投标产品或服务属于国家实行许可证制度或生产注册证制度的产品或服务，则应具备相应有效的证书。

若投标产品属于进口产品，则应按照《政府采购进口产品管理办法》（财库[2007]119号）文件和《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）文件办理。

3.2.2投标人应保证所提供的产品或服务免受第三方提出侵犯其知识产权（专利权、商标权、工业设计权及使用权等）的索赔或起诉，否则由此可能产生的一切法律责任和经济责任均由投标人承担。

4、投标费用

4.1 无论投标结果如何，投标人自行承担所有与参加投标有关的全部费用。

5、信息公告媒体

5.1浙江政府采购网(zfcg.czt.zj.gov.cn)和宁波政府采购网(www.nbzfcg.cn)为政府采购监督管理部门指定的政府采购信息发布媒体。本次政府采购活动有关信息均在该网站上予以公布，公布信息视同送达所有潜在投标人。

**B 招标文件**

6、招标文件

6.1招标文件由招标文件总目录所列内容组成。

6.2投标人应详细阅读招标文件的全部内容。不按招标文件的要求提供的投标文件和资料，则可能被视为无效标而导致投标被拒绝。

6.3为保证招标的公平性，若招标文件的技术指标要求存在排他性或歧视性条款，请投标人核实后，应在公告期限届满之日起7个工作日内，以书面形式（加盖单位公章）向招标人提出质疑请求、理由及事实证据材料。

6.4投标人可在投标截止时间5日前，对招标文件如有疑问要求澄清的，可用书面形式通知招标人，招标人应用书面作答（包括网上公告形式）。如有必要，可将答复内容包括原提出的问题（但不标明问题查询的来源），以网上公告形式通告潜在投标人。

6.5招标人在投标截止时间前，可对招标文件做必要的澄清或修改，并在指定的政府采购信息发布媒体上发布补充公告。该澄清或者修改的内容为招标文件的组成部分。

6.6因6.4条款或6.5条款做出实质性澄清或修改影响投标人编制投标文件的，至投标截止时间不足15日的，应顺延推迟投标截止时间和开标时间，并在指定的政府采购信息发布媒体上发布补充公告。

**C 投标文件**

7、投标文件语言和计量单位

7.1投标文件应用中文书写。投标文件中所附或所引用的原件不是中文时，应附中文译本。

7.2投标文件中所使用的计量单位，除招标文件中有特殊要求外，应采用国家法定计量单位。

8、投标文件的制作

8.1 投标文件规格幅面（A4）应与正文一致，按照招标文件第六部分对投标文件格式部分规定的顺序，统一编目编码并编制目录。由于编排混乱导致投标文件被误读或查找不到，责任应当由投标人承担。

**8.2 制作电子投标文件的系统配置要求：64位的windows7及以上操作系统。**

**8.3潜在供应商应提前完成供应商注册，成为浙江省政府采购网(zfcg.czt.zj.gov.cn)正式供应商，并完成CA数字证书办理（CA驱动和申领流程：浙江政府采购网 > 下载专区 > 电子投标客户端 > CA驱动和申领流程）。因未注册入库、未办理CA数字证书等原因造成无法投标或投标失败等后果由供应商自行承担。**

8.4供应商通过政采云电子交易客户端（下载位置：浙江政府采购网 > 下载专区 > 电子投标客户端 > 政采云电子交易客户端）制作电子加密投标文件（后缀jmbs），按“供应商-电子交易操作手册.pdf”及本招标文件规定的格式和顺序编制并进行关联定位、加密并在投标截止时间前上传。在生成加密投标文件同时会生成备份投标文件（后缀为bfbs）。备份投标文件是否提交由供应商自行决定。电子投标文件内容应与备份投标文件内容保持一致。

8.5电子投标文件未按时解密，投标人提供了备份投标文件的，以备份投标文件作为依据，否则视为投标文件撤回，备份投标文件将在评标室实时监控环境下拆封并导入政采云平台。电子投标文件已按时解密的，备份投标文件自动失效。

8.6投标人选择递交备份投标文件的，必须以U盘为存储介质。

8.7备份投标文件密封要求：外包装封面上应注明投标人名称、投标人地址、投标人联系方式（授权代表手机）、投标项目名称、项目编号、标项及“开标时启封”字样，并加盖投标人公章。

8.8 供应商在使用电子交易平台进行投标的过程中遇到涉及平台使用的任何问题，可致电政采云平台技术支持热线咨询，联系方式：95763（服务时间：工作日8：00-20：00）。

9、投标报价

9.1投标人要按投标产品数量、价格表的内容要求完整填写。

9.2对于非标准产品的投标，还应填报报价明细表（报价明细表格式由投标人自行设计）。

9.3所有投标均以人民币报价，投标人如需用外汇购入某些投标产品，须折合人民币计入总报价中，同时提供美金报价、折扣率、与人民币比值。

9.4除招标文件中有特殊规定外，招标人不接受任何选择报价，投标人对每一种产品只允许有一个报价。

9.5最低报价不能作为中标的保证。

10、投标文件的有效期

10.1在投标有效期内，投标文件应保持有效。

10.2在特殊情况下，招标人可与投标人协商延长投标标书的有效期，这种要求和答复都应以书面的形式进行，同意延长有效期的投标人不能修改投标文件。

11、投标文件的签署

投标文件应按招标文件第六部分对投标文件格式部分规定的要求进行签署。

**D投标文件的递交**

12、投标截止时间

投标文件须按照招标文件规定的投标时间上传。截至投标截止时间，电子投标通道将关闭，投标人未完成电子投标文件上传的，投标将被拒绝，备份投标文件将被拒收。

13、投标文件的补充、修改和撤回

13.1投标人在投标截止时间前，可对其所递交的投标文件进行补充、修改或者撤回。

13.2投标人在投标截止时间前需要对投标文件进行补充、修改的，应当使用投标文件制作工具重新制作并上传。供应商自行决定是否重新递交新的备份投标文件。

13.3备份投标文件由于包装不妥，在送交途中严重破损或失散的及未按规定密封或标记的将被拒收。

13.4在投标截止时间之后，投标人不得撤回投标。

**E 开标及评标**

14.开标评标过程中出现以下情形，导致电子交易平台无法正常运行，且无法保证电子交易的公平、公正和安全时，招标人可暂停电子交易活动：

14.1电子交易平台发生故障而无法登录访问的；

14.2电子交易平台应用或数据库出现错误，不能进行正常操作的；

14.3电子交易平台发现严重安全漏洞，有潜在泄密危险的；

14.4病毒发作导致不能进行正常操作的；

14.5其他无法保证电子交易的公平、公正和安全的情况。

出现前款规定情形，不影响采购公平、公正性的，招标人可以待上述情形消除后继续组织电子交易活动；影响或可能影响采购公平、公正性的，应当重新组织采购。

15.电子开标

15.1招标人在政采云平台主持电子开标。

15.1.1投标截止时间到，投标人不足3家，不进入标书解密开标程序。

15.1.2投标人须登录政采云平台在**投标截止时间后30分钟内**用制作加密投标文件的数字认证证书（**同一个CA证书**）完成投标文件解密工作，公布开标一览表内容。**解密结束时间后，系统自动关闭解密通道，供应商如按要求递交了备份投标文件的，将由项目负责人将备份投标文件导入政采云平台，视同完成投标文件解密工作。以下三种情形将被视作投标无效：一是仅提供备份投标文件的；二是电子投标文件解密失败，且未在规定时间内提交备份投标文件的；三是电子投标文件解密失败，虽然在规定时间内提交了备份投标文件，但是备份投标文件无法导入或者无法读取或者不符合本招标文件和电子交易平台要求的。**

15.2 需要参加项目现场讲标（答辩）的，授权代表应当参加，并在投标现场提供参加人员名单及身份证明材料。

16.对投标文件的初审

16.1初审内容为投标文件是否符合招标文件的要求、内容是否完整、有无计算错误，文件签署是否齐全。

16.2对价格错误，评审委员会按下述原则修正：

1. 开标一览表与分项报价表等投标文件相应内容不一致的，以开标一览表为准；
2. 大写金额与小写金额不一致的，以大写金额为准；
3. 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；
4. 总价金额与按单价汇总金额不一致的，以单价金额计算结果为准；

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价经投标人确认后产生约束力，投标人不确认的，其投标无效。

16.3投标文件内容有歧义或不一致的，按不利于投标人作出认定。

16.4招标人对投标文件的判定，只依据投标内容本身，不依靠开标后的任何外来证明。

17.讲标（答辩）及投标的澄清

17.1需要讲标（答辩）的，招标人工作人员应核对投标人讲标（答辩）人员，依次逐个带领投标人代表进出讲标（答辩）场所。

17.2招标人有权就投标文件中含混之处向投标人提出询问或澄清要求，投标人应当按照招标人通知的时间、地点进行答疑和澄清。

17.3必要时招标人可要求投标人就澄清的问题作书面回答，该书面回答应有投标全权代表的签章，并将作为投标内容的一部分。

17.4投标人对投标文件的澄清不得改变投标价格及实质内容。

18.比较及评价

18.1招标人根据招标产品特点组建评审委员会，对具备实质性响应的投标文件进行评估和比较。评审委员会由招标人、产品需求方、技术、经济、法律专家和其他有关方面的代表组成。

18.2评标标准及评标方法详细见招标文件第二部分。

19.评标过程保密

19.1开标之后，直到评标结束，凡是属于审查、澄清、评价和比较投标的有关资料以及授标意向等，均不得向投标人或其他无关的人员透露。

19.2在评标期间，投标人企图影响招标人的任何活动，将导致投标被拒绝，并承担相应法律责任。

**F 授予合同**

20、公示及定标

20.1评标结果公示。招标人在评标结束后，评标结果在政府采购监督管理部门指定媒体上公示，投标人可询问自身评审综合得分与排序。

20.2定标的形式有二种，一种是经采购人授权，由评审委员会直接确定中标方，另一种是由采购人对预中标进行审查确认中标方。

20.3接受最终审查的预中标方，应当予以配合并提供所需的有关资料。

21.招标人在授标时有变更数量的权力

在向投标人授予中标通知书时，招标人有权按有关规定变更数量和服务的内容。

22.中标通知

22.1在投标有效期内，招标人以书面形式（包括网站公布）通知所选定的中标方。

22.2中标通知书将是合同的一个组成部分。

23.签订合同

23.1中标方应按规定的时间、地点与买方签订中标经济合同，否则按开标后撤回投标处理。

23.2招标文件，中标方的投标文件及评标过程中有关澄清文件均应作为合同附件。

24.中标方如未按第23.1条的规定办理，招标人有权撤销其中标资格。在这种情况下，招标人可另选中标方或另行招标。

**G 风险监督**

### 25.廉洁自律规定

25.1集中采购机构工作人员不得与采购人、供应商恶意串通。

25.2集中采购机构工作人员不得接受采购人或者供应商组织的宴请、旅游、娱乐，不得收受礼品、现金、有价证券等，不得向采购人或者供应商报销应当由个人承担的费用。

### 26.人员回避

潜在投标人认为招标文件使自己的权益受到损害的，投标人认为采购人员及其相关人员有法律法规所列与其他供应商有利害关系的，可以向集中采购机构书面提出回避申请，并说明理由。

### 27.质疑的提出与接收

27.1投标人认为采购文件、采购过程和中标结果使自己的权益受到损害的，可以根据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》和《政府采购质疑和投诉办法》的有关规定，依法提出质疑。对采购文件需求的质疑以书面形式向采购人提出，对采购文件其他内容的质疑以书面形式向采购人和采购代理机构提出；对采购过程和中标结果以书面形式向采购代理机构提出质疑。

27.2质疑供应商应按照财政部制定的《政府采购质疑函范本》格式（可从www.ccgp.gov.cn网站下载）和《政府采购质疑和投诉办法》的要求，在法定质疑期内以书面形式提出质疑，针对同一采购程序环节的质疑应一次性提出。

超出法定质疑期提交的质疑将被拒绝。

重复或分次提出的、内容或形式不符合《政府采购质疑和投诉办法》的，质疑供应商将依法承担不利后果。

27.3质疑函接收联系人、联系电话和通讯地址见投标资料表。

**第五部分 合同格式**

**项目合同**

**合同编号：**

**甲方：**

**乙方：**

为保证 的顺利建成，甲方通过公开招标采购（招标编号： ）确定 为中标单位。双方依据《中华人民共和国民法典》，本着友好合作、平等互利的原则，经协商一致，特签订本合同，共同遵守执行。合同具体内容如下：

1. **项目名称**

1. **服务内容**

1. **履行的计划**

1. **费用和支付方式**

1. **双方责任与义务**
2. 甲方的责任、权利和义务

1. 乙方的责任、权利和义务

1. **项目变更**

1. **保密要求**

1、 甲方提供给乙方的信息中，除根据国家有关法律及甲方书面确认可以公开的以外，均属保密范围。对于与执行本合同相关的信息、业务流程和文件，未经甲方书面同意，乙方及其与执行本合同有关的人员不得直接或间接地向任何其他方有意或无意识地披露或泄露。已通过其他方式广为人知的信息与文件除外。甲方上级主管部门或者司法部门要求乙方提供上述文件时亦除外，但是乙方应该就此及时通知甲方。不论本合同是否变更、解除或终止，本条款均有效。

2、 乙方在接受甲方的委托事项后，应当做好保密准备，自接到甲方提供的第一份保密资料起，即应采取严格有效的保密措施，及时将保密资料与其他文件、资料进行分离保管；乙方不得利用所掌握的甲方保密资料营利；乙方未经甲方书面同意，不得擅自转让本协议的任何责任及其任何义务于任何第三方。

3、 乙方参与本项目咨询服务工作的所有人员均应遵从本协议之条款；若以上人员出现泄密行为，乙方应承担全部违约责任。

1. **人力不可抗拒事故**

因台风、地震、水灾、政府政策变化以及其它非双方责任造成的，不能预见、不能避免、并不能克服的客观情况为不可抗力。遇有不可抗力的一方，应立即将事件情况通知对方，并在15天内提供事件详情以及合同不能履行，或部分不能履行，或需要延期履行的理由的有效证明文件，按事件对履行合同的影响程度，由双方协商决定是否解除合同、部分免除履行合同的责任或延期履行。

1. **争议的解决与违规责任**

1．在本合同履行过程中发生争议，双方应当友好协商解决。如协商不成，申请宁波仲裁委员会仲裁解决。

2．在合同争议的协商、调解仲裁及起诉等过程中，双方仍应继续承担各自的责任和义务，保证工程建设的正常进行。

3．本合同对于甲、乙双方具有同等约束效力。除因受《中华人民共和国民法典》规定的不可抗力因素影响外，因一方责任导致合同不能正常履行的，视作其违约，违约方应当赔偿另一方的损失，损失赔偿额应当相当于因违约所造成的损失，包括合同履行后可以获得的利益，但不得超过违反合同一方订立合同时预见到或者应当预见到的因违反合同可能造成的损失。

1. **其他事项**

1．当甲方要求乙方扩大其工作范围，或者增加其工作时间，或者延长本合同执行有效期的，双方应另行协商并签订补充协议或合同。

2．合同的变更及其补充协议将以书面形式为准，是本合同的组成部分，具有同等的法律效力。

3．本合同一式 份，甲方执 份，乙方执 份。

4．合同未尽事宜，双方另行协商。

甲方（盖章）： 乙方（盖章）

地址： 地址：

法定（授权）代表人： 法定（授权）代表人：

日期： 年 月 日 日期： 年 月 日

**第六部分 投标文件格式**

封面

**投**

**标**

**文**

**件**

采购编号:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

项目名称:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

投 标 人:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

年 月 日

**投标应答索引表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 项目 | 投标人应答内容 | 对应页码 | 备注 |
| 一 | **报价部分** | / | / | / |
| 1 | 投标函 | 有 |  |  |
| 2 | 开标一览表 | 有 |  |  |
| 3 | 投标分项报价表 | 有 |  |  |
| 4 | 投标报价合理性说明 | 有或没有 |  |  |
| 5 | 其他报价资料 | 有或没有 |  |  |
| 二 | **商务技术部分** | / | / | / |
| 1 | 技术（商务/服务）规范偏离表 | 有 |  |  |
| 2 | 售后服务表 | 有 |  |  |
| 3 | 完成的类似项目一览表 | 有或没有 |  |  |
| 4 | 实施/技术人员一览表 | 有 |  |  |
| 5 | 其他商务技术资料 | 有或没有 |  |  |
| 三 | **资格响应部分** | / | / | / |
| 1 | 特定资格条件证明材料 | 有或没有 |  |  |
| 2 | 营业执照、事业或社团登记证等副本 | 有 |  |  |
| 3 | 法定代表人授权书 | 有，或没有 |  | 授权他人的需要提供 |
| 4 | 法定代表人、被授权人身份证明 | 有 |  |  |
| 5 | 分包意向承诺 | 有或没有 |  |  |
| 6 | 诚信投标承诺书 | 有 |  |  |
| 7 | 中小企业声明函 | 有 |  |  |
| 8 | 残疾人福利性单位声明函 | 有或没有 |  |  |
| 9 | 制造厂商授权函 | 有或没有 |  |  |
| 10 | 其他资格证明资料 |  |  |  |

**一、报价部分**

**1、投标函**

致：宁波市政府采购中心

我方参加贵方组织*项目名称(*采购编号XXXXX*)*招标的有关活动，并进行电子投标。据此函，我方宣布同意如下：

1. 提供投标须知规定的全部电子投标文件，上传到“政采云”平台。
2. 投标报价详见开标一览表。
3. 已详细审查全部招标文件，包括修改文件（如有的话）以及全部参考资料和有关附件，我方完全理解并同意放弃对这方面有不明及误解的权利。
4. 保证遵守招标文件中的有关规定，承担规定的责任义务。
5. 提供按照贵方可能要求的与其投标有关的一切数据或资料，完全理解贵方不一定接受最低价的投标或收到的任何投标。
6. 投标文件内容有歧义或不一致的，同意按不利于我方作出解释。
7. 投标有效期：90天。

与本投标有关的一切往来通讯方式：

投标单位全称：

地址： 邮编：

联系人： 电话： 传真：

移动电话： 电子邮件：

投标单位（**盖章**）：

法定代表人或其委托代理人（**签字或签章**）：

日期：

可先进行纸质打印，代表签字或签章后，再进行扫描提交。**2、开标一览表**

项目名称：XXXX 采购编号：XXXX

|  |
| --- |
| 投标总价合计人民币（小写）：￥  投标总价合计人民币（大写）： |
| 工期：合同签订后至 年 月通过采购人验收。 |

投标单位全称**（盖章）**：

日期：

**3、投标分项报价表**

项目名称： 采购编号： （人民币：元）

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 品目名称 | 品牌（生产/服务商） | 规格型号及配置（或服务内容） | 产地 | 数量 | 数量  单位 | 市场平均单价 | 投标单价 | 投标总价 | 备注 |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 合计 | / | / | / | / |  | / | / | / |  |  |

*说明：1、产地为境内的请填写设区市、地市级地区名称，允许进口产品投标的境外产品方可填写国家或地区名称（含港澳台地区）；工程和服务的产地是指生产商所在地，货物的产地是指整机（非零部件）最终生产地点。*

1. *市场平均单价是指该同等配置产品在近期国内市场实际销售的平均价格，投标单价不得高于市场平均单价。*

投标单位全称**（盖章）**：

日期：

**4、投标报价合理性说明**

投标人自行提供报价合理性说明，必要时提交相关证明材料，相关材料内容及格式由投标人自行拟定。

**5、其他报价资料**

投标人可结合招标文件及自身情况提供其他认为必要的资料。**二、商务技术部分**

**1、技术（商务/服务）偏离表**

项目名称： 采购编号：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 品目/内容 | 招标要求 | 投标响应 | 对应页码 | 偏离情况 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

特别说明：技术偏离不得笼统提供，必须按招标文件要求逐条填报，并按要求提供技术支持证明资料所对应页码，投标响应与招标要求完全一致的才能填写“无偏离”、其他应当如实分别填写“正偏离”或“负偏离”。

投标单位全称**（盖章）**：

日期：

**2、售后服务表**

项目名称： 采购编号：

|  |  |
| --- | --- |
| 售后服务内容 | 1.  2.  3. |

投标单位全称**（盖章）**：

日期：

## **3、完成的类似项目一览表**

项目名称： 采购编号：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 项目名称 | 项目时间  年/月 | 使用单位名称、地址及联系方式 | 项目合同金额（单位：万元） | 证明材料对应页码 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 |  |  |  |  |  |

投标单位全称**（盖章）**：

日期：

## **4、实施/技术人员一览表**

项目名称： 采购编号：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 姓名 | 拟担任的职务 | 身份证号码 | 同类项目工作经历 | 证明材料对应页码 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 |  |  |  |  |  |

投标单位全称**（盖章）**：

日期：

**5、其他商务技术资料**

投标人可结合招标文件及自身情况提供其他认为必要的资料。

**三、资格响应部分**

**1、特定资格条件证明材料**

投标人可结合招标文件及自身情况提供必要的资料。

**2、营业执照、事业单位、社团组织、民办非企业等登记证副本扫描件**

**3、法定代表人授权书**

致：宁波市政府采购中心

XXXXX（投标单位全称）法定代表人XXX （姓名）XXXXX（身份证件号码）授权XXX（姓名、职务）XXXXX（身份证件号码）为委托代理人，参加贵方组织的 XXXX 项目（采购编号XXXXX）政府采购活动，全权处理政府采购活动中的一切事宜。

本授权书于XXXX年XX月XX日签署生效，特此声明。

投标单位全称（**盖章**）：

法定代表人（**签字或签章**）：

日期：

**注：**

**1.法定代表人作为投标授权代表的,本表无需提供；**

**2.分公司参加投标需经总公司授权许可，法定代表人授权书可改为分公司营业执照上登记的分公司负责人签字或签章；**

**3.电信、银行、保险等实行许可证属地经营的本地分公司可以直接参加许可证范围内项目投标，法定代表人授权书可改为分公司营业执照上登记的分公司负责人签字或签章，参加非许可证范围内项目投标的，需经总公司授权许可；**

**4.本授权书填写完成后可先进行纸质打印，经盖章、法定代表人签字或签章后，以扫描件形式提交。**

**4、法定代表人、被授权人身份证明扫描件**

1、法定代表人身份证扫描件：

|  |
| --- |
| 正面： 反面： |

2、授权代表身份证扫描件：（如法定代表人直接参加投标并对投标文件中的相应材料签字的，则无需提供）

|  |
| --- |
| 正面： 反面： |

**注：（1）法定代表人为投标授权代表的只需提供法定代表人身份证明；**

**（2）身份证明请提供身份证正反面扫描件或其他证件扫描件。**

**5、分包意向承诺**

（投标人名称）若成为宁波市政务信息化网络数据安全一体化指挥系统建设项目（项目编号：NBZFCG2023C026G）的中标供应商，将依法采取分包方式履行合同，拟接受分包的供应商为 □中型企业，□小型企业，□微型企业（如暂无法确定，可多选，如勾选中型企业，则不能享受价格分扣除优惠政策），分包合同金额占合同总金额的 %，分包工作內容包括 。

接受分包的小微企业与分包企业之间□不存在/□存在/□暂不确定直接控股、管理关系，暂不确定或存在直接控股、管理关系的不享受价格扣除优惠政策。

分包供应商不得再次分包或非法转包。

投标单位**（盖章）**：

日 期：

6**、诚信投标承诺书**

宁波市政府采购中心：

我方愿意参与“XXX项目（采购编号：XXX）”的投标，并作出如下承诺：

1、我方符合政府采购法第22条规定的条件，且在本项目公告日前3年内没有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（认定标准按《财政部关于<中华人民共和国政府采购法实施条例>第十九条第一款“较大数额罚款”具体适用问题的意见》（财库〔2022〕3号））等行政处罚的重大违法记录。

2、与采购人XXX（**填“有/无”**）关联，没有采取任何影响公平投标的行为。

3、在招投标过程中，不做以下任何事项：

（1）投标截止时间后撤回投标（包括开标后拒绝应当进行的讲标演示）；

（2）投标文件中提供虚假材料或不实材料；

（3）与其他投标人达成可能限制竞争的协议；

（4）为影响投标而向有关招标当事人提供金钱、物质及服务；

（5）与其他投标人围标、陪标；

（6）其他任何串通投标行为。

4、保证所投产品来自合法的供货渠道。

5、若中标后，保证按照投标承诺及时签订合同并履约。

我方若违背以上承诺，接受在政府采购指定媒体上公告曝光处理，同时承担依据国家法律法规追究的其他责任。

投标单位**（盖章）**：

日 期：

**特别说明：本承诺书不得实质性改动，否则视为无效标。**

**7、中小企业声明函**

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，本单位参加XXXXXX项目（采购编号XXXX）采购活动，郑重声明提供的服务全部由符合政策要求的中小企业承接，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）具体情况如下：

1. ***业务应用层建设***，所属行业为***软件和信息技术服务业***；服务商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
2. ***应用支撑层建设***，所属行业为***软件和信息技术服务业***；服务商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
3. ***数据资源层建设***，所属行业为***软件和信息技术服务业***；服务商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
4. ***数据库监测系统建设***，所属行业为***软件和信息技术服务业***；服务商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
5. ***数据库权限系统建设***，所属行业为***软件和信息技术服务业***；服务商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
6. ***机房安全监管建设（仅机房基础设施管理平台）***，所属行业为***软件和信息技术服务业***；服务商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
7. ***管理终端操作系统***，所属行业为***软件和信息技术服务业***；服务商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
8. ***安全防护系统***，所属行业为***软件和信息技术服务业***；服务商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
9. ***文档处理软件***，所属行业为***软件和信息技术服务业***；服务商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
10. ***办公软件***，所属行业为***软件和信息技术服务业***；服务商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
11. ***移动端PAD***，所属行业为***工业***；制造商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
12. ***工业级二维码打印机***，所属行业为***工业***；制造商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
13. ***管理终端***，所属行业为***工业***；制造商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
14. ***温度感知系统***，所属行业为***工业***；制造商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
15. ***UWB定位系统***，所属行业为***工业***；制造商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
16. ***防火墙***，所属行业为***工业***；制造商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
17. ***Web应用安全检测系统***，所属行业为***工业***；制造商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
18. ***操作系统***，所属行业为***软件和信息技术服务业***；服务商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
19. ***应用中间件***，所属行业为***软件和信息技术服务业***；服务商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、微型）*企业；
20. ***数据库管理软件***，所属行业为***软件和信息技术服务业***；服务商为*（企业名称）*，上年末从业人员*XXX*人，上年营业收入*XXX*万元，上年资产总额*XXX*万元，属于*（中型、小型、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。

本单位对上述声明的真实性负责。如有虚假，依法承担相应责任。

 投标单位名称**（盖章）**：

日  期：

填写说明：

1、以下情形不影响声明有效性，也不作为虚假资料情形：一是划型标准中行业不涉及的指标未填写或填写错误的；二是声明函所列行业与采购文件所明确行业不一致且不改变划型结果的；三是非企业供应商错误提交声明函的。

2、**项目专门面向中小企业采购的，投标人必须按要求提供本表，且投标货物和服务必须全部由中小企业制造或者承接。如有虚假，将对投标人按虚假材料谋取中标论处。**

3、**项目不是专门面向中小企业采购的，投标产品中有小微企业制造的货物（或者承接的服务）需要参照享受价格评分优惠的，投标人应仔细核实小微企业相关数据后提供本表。本表如有虚假，联合体或者分包方式的所有参与方均按虚假材料谋取中标论处，自行提供或者外购方式的以投标人虚假材料谋取中标论处。对相关制造商信息了解不充分，或者不能确定相关信息真实、准确的，不建议出具《中小企业声明函》。**

4、依据工业和信息化部、国家统计局、国家发展和改革委员会、财政部《关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）规定，具体企业行业分为：农林牧渔业，工业（包括采矿业，制造业，电力、热力、燃气及水生产和供应业），建筑业，批发业，零售业，交通运输业（不含铁路运输业），仓储业，邮政业，住宿业，餐饮业，信息传输业（包括电信、互联网和相关服务），软件和信息技术服务业，房地产开发经营，物业管理，租赁和商务服务业，其他未列明行业（包括科学研究和技术服务业，水利、环境和公共设施管理业，居民服务、修理和其他服务业，社会工作，文化、体育和娱乐业等）。一般研发、生产、加工型企业填写工业，销售、贸易型企业填写批发业，具体行业划分依据国家统计局网站公布的《国民经济行业分类》标准规定。各行业企业划型标准：

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

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

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

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

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

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

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

（8）邮政业。从业人员1000人以下或营业收入30000万元以下的为中小微型企业。其中，从业人员300人及以上，且营业收入2000万元及以上的为中型企业；从业人员20人及以上，且营业收入100万元及以上的为小型企业；从业人员20人以下或营业收入100万元以下的为微型企业。

（9）住宿业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入2000万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（10）餐饮业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入2000万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（11）信息传输业。从业人员2000人以下或营业收入100000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（12）软件和信息技术服务业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员10人及以上，且营业收入50万元及以上的为小型企业；从业人员10人以下或营业收入50万元以下的为微型企业。

（13）房地产开发经营。营业收入200000万元以下或资产总额10000万元以下的为中小微型企业。其中，营业收入1000万元及以上，且资产总额5000万元及以上的为中型企业；营业收入100万元及以上，且资产总额2000万元及以上的为小型企业；营业收入100万元以下或资产总额2000万元以下的为微型企业。

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

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

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

**中型企业标准上限即为大型企业标准下限。无上年度数据的新成立企业暂以当前实际数据填报。从业人数包括与企业订立劳动合同的职工人数和企业接受的劳务派遣用工人数。以分公司投标的，须填写法人公司的企业划型。**

5、联合体投标的，由联合体牵头方提供本表。

6、符合《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）规定的条件并提供提供《残疾人福利性单位声明函》的残疾人福利性单位视同小型、微型企业；根据《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）的规定，投标人提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业证明文件的，视同为小型、微型企业。

8**、残疾人福利性单位声明函**

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加“XXXX项目（采购编号：XXXX）”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。

投标单位名称**（盖章）**：

日  期：

填写说明：

1、本声明是残疾人福利性单位的提供，其他单位无需提供。

2、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）。

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者服务协议的雇员人数。

**9、制造厂商授权函（若有，扫描件）**

致：宁波市政府采购中心

我们*（制造商名称）*是按*中华人民共和国*法律成立的一家制造商，主要营业地点设在*（制造商地址）*。兹指派按中华人民共和国法律正式成立的，主要营业地点设在*（投标人地址）*的*（投标人名称）*作为我方真正的和合法的代理人进行下列有效的活动：

1. 代表我方办理贵方*（采购编号）*招标项目的投标邀请要求提供的由我方制造的产品的有关事宜，并对我方具有约束力。
2. 作为制造商，我方保证以投标合作者来约束自己，并对该投标共同和分别承担招标文件中所规定的义务。
3. 我方兹授予*（投标人名称）*全权办理和履行上述我方为完成上述各点所必须的事宜，具有替换或撤销的全权。兹确认*（投标人名称）*或其正式被授权代表依此合法地办理一切事宜。

制造商（公章）：

签字人姓名及职务：

签字人（签名）：

**10、其他资格证明资料**

投标人可结合招标文件及自身情况提供其他认为必要的资料。

第七部分 其他文件格式

**履约保证金保函**

**（若采用保函的，在中标后开具提交采购人）**

致：宁波市政府采购中心

本保函是我行（ [银行全称]）为 （以下简称卖方）根据贵处组织的 项目（采购编号 ）招标结果，将与 （以下简称买方）签订的经济合同及执行合同提供的担保。保证金金额为（大写人民币） 元。

当我行在收到贵处说明卖方违约的书面通知后，在20天内按通知要求金额无条件地支付给买方。

本保函的有效期为自开出之日起，至合同履约结束之日止。

银行全称：

（盖章）

开具人（签字）：

职务：

日期：