公开招标采购文件

项目编号：ZJZC-253055

项目名称：信息化设备及安全服务外包项目

采购单位：宁波市公路与运输管理中心

代理机构：浙江中创招投标有限公司

浙江中创招投标有限公司

二〇二五年三月

温馨提醒

1、投标文件应按采购文件要求将“资格文件”、“商务和技术文件”、“报价文件”分别编制。

2、采购人可以对已发出的采购文件进行必要的澄清或者修改，将以“更正公告”的形式发布在政采云平台，供应商应及时登录政采云平台，进行浏览并下载，未及时浏览下载的责任自负。

目　录

第一章　公开招标采购公告

项目概况

信息化设备及安全服务外包项目招标项目的潜在投标人应在政府采购云平台（http://www.zcygov.cn/）获取（下载）招标文件，并于2025年04月07日14：00（北京时间）前递交（上传）投标文件。

一、项目基本情况：

项目编号：ZJZC-253055

项目名称：信息化设备及安全服务外包项目

预算金额（元）：1268300

最高限价（元）：1268300

采购需求：

标项名称：信息化设备及安全服务外包

数量：1项

预算金额（元）：1268300

简要规格描述或项目基本概况介绍、用途：主要包括信息资产统计服务、运维管理建设服务、服务器运维服务、存储设备运维服务、网络设备运维服务、安全设备运维服务、机房设备运维服务、桌面终端运维服务等内容，具体内容见第二章采购需求。

备注：/

合同履约期限：标项1，自合同生效之日至合同全部权利义务履行完毕之日止。

本项目（否）接受联合体投标。

二、申请人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；

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

3.落实政府采购政策需满足的资格要求：本项目专门面向中小企业采购，供应商应为中小微企业、监狱企业、残疾人福利性单位；

4.本项目的特定资格要求：无。

三、获取招标文件：

1.时间：2025年03月18日至2025年03月25日，每天上午00：00至12：00，下午12：00至23：59（北京时间，线上获取法定节假日均可，线下获取文件法定节假日除外）

2.地点（网址）：政府采购云平台（http://www.zcygov.cn/）

3.方式：在线获取3.1、本项目采购文件实行“政府采购云平台”在线获取，不提供采购文件纸质版。供应商获取采购文件前应先完成“政府采购云平台”的账号注册；3.2、潜在供应商登录政采云平台，在线申请获取采购文件（进入“项目采购”应用，在获取采购文件菜单中选择项目，申请获取采购文件；3.3、招标公告附件内的采购文件仅供阅览使用，投标人只有在“政府采购云平台”完成获取采购文件申请并下载了采购文件后才视作依法获取采

购文件(法律法规所指的供应商获取采购文件时间以供应商完成获取采购文件申请后下载采购文件的时间为准）。注：请投标人按上述要求获取采购文件，如未在“政采云”系统内完成相关流程，引起的投标无效责任自负。

四、提交投标文件截止时间、开标时间和地点：

提交投标文件截止时间：2025 年 04 月 07 日 14：00（北京时间）

投标地点（网址）：政采云平台（https：//www.zcygov.cn/）

开标时间：2025 年 04 月 07 日 14：00（北京时间）

开标地点（网址）：政采云平台（https：//www.zcygov.cn/）

五、公告期限：自本公告发布之日起 5 个工作日。

六、其他补充事实：

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.其他事项：2.1、供应商应于**提交投标文件截止时间**将电子投标文件上传到政府采购云平台 www.zcygov.cn，逾期或未成功上传电子投标文件，视为供应商放弃投标。2.2、采用邮寄方式递交电子备份投标文件的，请留足邮寄时间，递交时间以邮寄签收时间为准，**提交投标文件截止时间**邮寄至本公告第四条所述采购代理机构处。投标人邮寄后请电话或电子邮箱（tender06@126.com）提供邮寄信息给采购代理机构，以便及时确认送达情况。邮寄延误送达或未密封将予以拒收，采购代理机构无责确保文件及时接收，相关责任与后果全部由投标人自行承担。2.3、采用现场递交电子备份投标文件，投标人代表于**提交投标文件截止时间**送达开标现场（宁波市环城西路北段 225 号真如中心 15 楼浙江中创招投标有限公司开标室），电子备份投标文件需密封，逾期送达或未密封的将予以拒收。2.4、供应商仅提供备份投标文件的，但未在投标截止时间前成功上传电子加密投标文件者，其全部投标文件无效。2.5、特别说明：（1）“电子备份投标文件”应为投标人通过“政采云”系统生成的本项目“电子加密投标文件”对应的数据电文形式的电子文件并以介质存储的方式（U 盘）（以下简称电子备份投标文件），该“电子备份投标文件”只有在投标人成功上传“电子加密投标文件”，但无法读取时或在解密时间内无法解密或解密失败时，方可调用“电子备份投标文件”，否则不予调用电子备份投标文件。电子备份投标文件损坏、格式不符等致使异常情况处理失败的责任由投标人自行承担。（2）采购代理机构将在采购文件规定的时间通过政府采购云平台组织开标、开启投标文件，所有供应商均应准时在线参加。开标时间后 30 分钟内供应商可以登录政府采购云平台 www.zcygov.cn，用“项目采购-开标评标”功能进行解密投标文件。若供应商在规定时间内（开标时间后 30 分钟内）无法解密或解密失败，可使用电子备份投标文件进行电子评标。2.6、本项目实行网上投标，采用电子投标文件。若供应商参与投标，自行承担投标一切费用。2.7、标前准备：各供应商应在开标前确保成为浙

江政府采购网正式注册入库供应商，并完成CA数字证书办理。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。CA数字证书相关操作可参考“浙江政府采购网-下载专区-电子交易客户端-CA驱动和申领流程”2.8、投标文件制作：（1）应按照本项目采购文件和政府采购云平台的要求编制、加密并递交投标文件。供应商在使用系统进行投标的过程中遇到涉及平台使用的任何问题，可致电政府采购云平台技术支持热线咨询，联系方式：95763。（2）供应商通过政府采购云平台电子投标工具制作投标文件，电子投标工具请供应商自行前往浙江政府采购网下载并安装（下载网址：http://zfcg.czt.zj.gov.cn/bidClientTemplate/2019-05-27/12946.html），投标文件制作具体流程详见政府采购云平台“供应商-政府采购项目电子交易操作指南”（https://help.zcygov.cn/web/site_2/2018/12-28/2573.html）。（3）以U盘存储的电子备份投标文件1份，按政府采购云平台要求制作的电子备份文件，以用于异常情况处理。2.9、落实的政策：《关于促进残疾人就业政府采购政策的通知》（财库[2017]141号）、《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）、《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）。2.10、本次政府采购活动有关信息在“浙江政府采购网（http://zfcg.czt.zj.gov.cn/）”、“宁波市政府采购网（www.nbzfcg.cn）”网站上公布，公布信息视同送达所有潜在投标人。

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：宁波市公路与运输管理中心

地　　址：宁波市鄞州区姚隘路845号

传　　真：/

项目联系人（询问）：朱老师

项目联系方式（询问）：0574-55129727

质疑联系人：刘老师

质疑联系方式：0574-87920787

2.采购代理机构信息

名称：浙江中创招投标有限公司

地址：宁波市环城西路北段225号真如中心15楼

传真：0574-87179089、邮箱：tender06@126.com

项目联系人（询问）：夏坤、张百军、王家兴、卢杭燕、张晓亮、吴凤珠

项目联系方式（询问）：0574-87179082

质疑联系人：周俊辉

质疑联系方式：0574-87179087

3.同级政府采购监督管理部门

名称：宁波市财政局政府采购监管处

地址：宁波市中山西路19号

联系人：李老师

监督投诉电话：0574-89388042

温馨提示：

若对项目采购电子交易系统操作有疑问，可登录政采云（https：//www.zcygov.cn/），点击右侧咨询小采，获取采小蜜智能服务管家帮助，或拨打政采云服务热线95763获取热线服务帮助。

第二章　采购需求

一、项目概况

（一）IT 维护技术服务项目内容：

信息资产统计服务、运维管理建设服务、服务器运维服务、存储设备运维服务、网络设备运维服务、安全设备运维服务、机房设备运维服务、桌面终端运维服务等内容。

（二）服务地点及范围

1、路网大楼

序号	设备名称	数量
1	桌面设备，办公电脑，及打印机等桌面周边设备	约 40 台
2	核心机房 IT 设备包含服务器，存储，网络设备等	总数约 170 台
3	UPS 系统（需提供配件包含电池组更换服务）	3 套（路网中心机房 2 套，3 楼指挥中心 1 套）
4	精密空调（每年提供两次精密空调外机清洗服务，及空调过滤网更换服务。）	4 台
5	机房基础设备,包含消防系统，机房内部安防系统，环境动力监控系统，机房照明系统，路网中心综合布线系统。	1 套
6	针对公路运输中心一批需充放电的设备进行定期充放电维护，（需提供锂电池的更换服务）	239 台
7	对路网中心视频会议终端设备进行运维，包括专业巡检、系统调优、数据维护、重大事件现场支持。对会场话筒、大屏、音响、大屏系统、线缆等辅助设备进行日常运维，对损坏的设备进行维修更换。涉及路网中心视频会议设备日常运维、设备运维等。无偿提供具有原厂或与原厂同等级的技术支持。	1 套

2、中心大楼

序号	设备名称	数量
1	桌面设备，办公电脑，及打印机等桌面周边设备	约 130 台
2	机房 IT 设备主要有网络设备等	总数约 10 台
3	UPS 系统	1 套
4	精密空调	2 台
5	机房基础设备,包含消防系统，机房照明系统，综合布线系统。	1 套

3、路政大楼

序号	设备名称	数量
1	桌面设备，办公电脑，及打印机等桌面周边设备	约 150 台
2	机房 IT 设备主要有网络设备等	总数约 10 台
3	UPS 系统	1 套
4	精密空调	1 台
5	机房基础设备,包含消防系统，机房照明系统，综合布线系统。	1 套

4、高速公路视频资料整合平台（10 个下属单位）

序号	设备名称	数量
1	海康威视 DVR 等视频周边设备	约 20 台

5、路网中心 GQY 大屏延保服务

序号	设备名称	数量
1	72 英寸 DLP 大屏	32 块
2	大屏控制管理软件	1 套
3	高分应用平台（含多媒体接入、交通综合管理可视化信息）	1 套

6、信息安全运维外包服务

序号	服务内容	数量
1	宁波市公路与运输管理中心信息安全运维服务	1 项

注：以上运维中涉及的产品均需提供配件更换服务，配件更换费用由中标方承担，用户无需再支付费用。

（三）服务期限：

一年。

二、运维方式及人员要求

本项目投入的人员要求：须为本单位在职人员，需提供开标日前近三个月投标人为其专职人员缴纳的社保证明、有专职人员相关证书，所有证明资料须编入投标文件内。

所配备的人员必须编入投标文件“项目人员配置表”内。具体拟派人员要求如下：

1、针对中心大楼、路政大楼、路网大楼的数据中心机房及桌面端维护，供应商需分别各驻场 1 名外包服务工程师。1 名机动工程师，负责 10 个高速公路业主公司及中心关联企业内中心所属信息化设备的运维服务。

2、针对信息安全运维服务供应商需指定驻场 1 名具有中国信息安全测评中心认证的注册信息安全管理人员证书及工信部网络工程师证书的安全运维工程师。

3、为确保调度大屏的正常运行，针对路网中心 GQY 大屏延保服务供应商应提供 1 名技术工程师实现 24 小时应急响应服务。

4、项目团队须配备一名项目负责人总体负责本项目的管理和协调，项目负责人须有 3 年以上信息化领域从业经历，常驻宁波。项目负责人应覆盖硬件设备运维管理的相关技术领域，包括服务器、存储、网络和安全设备、数据库等。

5、项目团队须制定一名项目技术负责人，项目技术负责人应覆盖硬件设备运维管理的相关技术领域，包括服务器、存储、网络和安全设备、数据库等。

6、项目团队须指定一名项目投诉处理人（非项目协调人），以完成本项目的质量监控，提供联系电话。针对项目投诉必须在 24 小时内给出书面答复。

7、对于中标单位派驻的驻场服务人员及机动人员，如不满足用户的人员要求，用户有权要求更换人员，直到符合用户需求为止。原则上已符合用户要求的的派遣人员，中标单位不得随意更换，如确因故调换已有运维人员，中标单位须在实施调换前 15 个工作日书面通知用户，在征得用户同意的情况下方可进行调整，调换后的运维人员技术水平不得降低。

三、具体运维服务要求

（一）信息资产统计服务

1、维保服务内容：

通过 IT 运维系统建立完善的设备档案(包含在运维数据库中），为以后的配置的变更管理和其他 IT 维护服务的顺利进行打下良好的基础。IT 运维系统资产管理应包括：

标记设备：计算机及外设设备、网络设备、安全设备服务器及存储等 IT 系统设备进行统一的资产登记，并建立唯一标号；

建立设备配置文档：网络设备、安全设备服务器及存储的配置信息进行记录和分析，建立硬件设备配置档案；

网络地址管理列表：IP 地址、子网地址、VLAN 进行统一的规划和分配，并建立管理文档。

（二）运维管理建设服务

为规范化宁波市公路与运输管理中心信息系统的运维和管理工作，协助用户建立整体性运维体系，规范运维流程管理、运维资料管理、运维事件管理、系统监控管理等过程。本项目要求供应商在服务期限内提供 IT 运维一体机服务，其技术参数要求如下：

指标项	指标要求
一、总体架构	
系统架构	采用 B/S 架构，支持中文管理界面。
部署方式	支持集中式和分布式部署方式，实现跨机房的数据中心运维监控。
	监控对象采用无代理方式部署，支持 SNMP、SSH、JMX 等采集模式，采集过程要求不影响监控对象的性能。
	可以作为数据中心服务平台单独使用，也可以作为运维云的线下服务终端使用。
权限	按不同用户角色，分配监控对象和视图查看权限，实现用户角色和监控对象、视图的查看权限关联
二、功能	
数据库监控	支持 Oracle、SQL Server、MySQL、DB2 等数据库。
	支持数据库运行健康状态监控，包括： 可用性监控：监听、实例、表空间的可用性； 错误监控：数据库运行过程中的错误数量； 性能监控：数据块逻辑读指标直观反映数据库性能； 变化监控：对象（表、索引、视图等）、权限（用户、表）、空间（对象、表空间、归档）的变化量； 可靠性监控：备份及容灾系统的运行状态。
	支持 SQL 执行生命周期完整监控，包括：登录、解析、执行、提交。 通过 SQL 执行次数、SQL 执行时间，主观展示 SQL 执行性能瓶颈。
	支持数据库关联资源监控，包括： 数据库资源监控：processes、session、DB files、jobs。 三大资源锁监控：Mutex、 Latch、 Lock。 主机资源监控，包括：CPU、内存、存储、网络。
数据库巡	支持 2 个对象的业务系统、数据库类型、实例名、操作系统、IP 地址、巡检完

检	成时间等信息进行全面巡检 支持巡检对象的异常信息数量统计，运维人员可及时掌控各系统数据库的健康状况整合资深数据库专家的多年运维经验，形成专家智能系统，根据数据库的健康状态，给出专业的分析，对数据库可能存在的故障和问题进行快速定位，对每个异常指标提供专业解读和排错建议 1.支持一键操作实现全面巡检 2.全面巡检的报告内容至少包括：数据库可用性、空间管理、安全性、可靠性、性能、错误、主机资源、数据库资源、数据库软件、数据库参数、系统参数等信息 3.支持在线和以 PDF 文档导出两种方式查看巡检报告
数据中心监控	支持 WebLogic、Tomcat 等主流业务中间件监控。采用 JMX 直接监控 Java 应用程序服务器的功能，无需第三方模块或集成层。使用高效的 Java 网关监视 Tomcat 等应用服务器，包括：JVM 可用内存、JVM 最大内存、JVM 总的内存、线程等。
	支持 Linux、Windows、AIX、HP-UX、Solaris 等操作系统监控。监控操作系统的运行状态，包括：主机状态、CPU 利用率、内存利用率、磁盘 I/O 读写速率、磁盘 I/O 读写速率，网络 I/O 等。
	支持 VMware 虚拟机状态监控，包括：VMware 物理主机硬件状态、虚拟机在线状态、CPU 利用率、内存大小及利用率、磁盘空间大小及利用率等。
	支持 IBM、HP、DELL、联想、曙光、浪潮等主流物理服务器监控，包括对服务器的硬件状态进行自动告警，包括：CPU、硬盘、电源、风扇、RAID 卡等。
	支持 EMC、NetApp、IBM、华为等主流存储设备监控，包括：存储系统的磁盘、存储控制器、电源、风扇等运行状态。
	支持华为、H3C、思科、锐捷等主流网络设备监控，包括监控网络设备的在线状态。对网络线路运行状态监控，包括线路连通性、线路响应时间、线路流量、线路带宽利用率、线路错包率、线路丢包率等信息。对网络设备接口状态进行监管，包括接口状态、接口流量性能等信息。
触发模式	支持人工阀值模式，可自由设置告警触发阀值库。 支持智能诊断模式，采用大数据技术和机器学习技术，智能识别异常，并发送警告。
监控视图	预先封装不同监控对象的大屏展示模版，包括：中间件、数据库、操作系统、虚拟机、物理服务器等。实现常见运维故障（80%以上）及隐患能从大屏中直观展示及告警。 支持按照业务角度进行关联视图定制。 支持按照资源种类进行分类和关联视图定制。 支持机柜图、系统拓扑图、网络拓扑图等视图定制。 其中数据库监控模版，要求实现： 1.一张大屏可以直观显示监控对象的健康指数，并根据阀值自动告警。 2.从流程及时间模型的角度联动展示各项指标，清晰定位问题环节。
运维云服务	提供和运维一体机配套的线上运维云服务，实现告警订阅、告警推送、工单流转、数据库专家在线服务等功能
	运维云服务采用多租户方式交付，不同租户之间安全隔离。 运维一体机采用加密通道方式和运维云单向连接。
	可定义告警推送和服务人员接收的对应关系，包括：告警站点、告警级别、通知方式等。
	按运维对象的重要性和故障级别，可定义不同的告警通知级别。 告警通知方式支持：邮件、微信、APP。 支持告警通知升级机制。

	提供待处理告警列表，服务人员快速查阅需要处理但还未处理的告警。 采用大数据结构的集中管理模式，支持告警日志的高效查询、分析。 告警日志保存时间要求至少 13 个月以上。
	提供新建工单、工单流转、工单升级、工单统计报表等功能。 与告警订阅和服务授权紧耦合。 针对“待处理告警”，支持一键发起服务工单。
	提供数据库巡检和 AWR 报告解读工具，支持离线上传采集包和 AWR 原生报告，自动生成巡检报告和 AWR 解读报告。
	可单独订购远程数据库专家服务。 通过把数据库告警同步推送给线上数据库专家，并上传诊断资料包，数据库专家结合告警内容和诊断资料包进行分析，给出解决方案和交付服务。
三、产品规格与授权	
产品形态	软硬件一体机方式
硬件指标	1U 机架式 内存≥8G 存储空间≥500G 至少提供 4 个网口
授权数量	支持 8 个数据库实例，100 个监控节点

（三）服务器运维

1、维保服务内容

本次维保包括现有清单所列服务器以及服务期内新增服务器的硬件维保服务，维保期间的故障部件更换费用由投标单位承担。

（1）日常维护

包含设备的检测、维护、维修、搬迁，以及操作系统安装、设备软硬件的配置调整、设备固件版本升级等。所需备品和耗材由中标方免费提供，提供人员驻点服务。

必须提供巡检项目记录表。巡检结束后由技术人员和招标单位指定人员签字，当场提交巡检记录表。

2、服务响应及服务人员

要求提供 7×24 小时服务，电话响应在 15 分钟以内，电话支持无法解决问题的情况下 1 小时内到达现场。确定为硬件故障需要更换的，在备件到位后 12 小时内解决故障问题。维护完成后当场提交服务报告，由服务人员和招标方指定人员签字确认。故障件更换需提交部件设备更换单，并载明原部件型号及序列号、更换部件型号及序列号等内容。

投标方需提供指定服务人员的资质、多种联系方式，未经招标方同意投标方不得随意调整指定服务人员。

（四）存储

1、维保服务内容

本次维保包括现有清单所列存储设备以及服务期内新增存储设备的软硬件维保服务以及定期巡检服务。

（1）主动运维服务

为减少存储故障对业务工作的影响，需要投标方提供主动运维服务，在招标方未发现故障的情况下能提前或主动发现存储存在的问题。

（2）软硬件日常维护

包含设备的检测、维护、维修、搬迁、以及存储空间的调整分配、数据迁移、数据备份、设备固件版本升级及其他软硬件配置等。

更换备件部件费用由投标单位承担，所供备件需为原厂，不得提供假货，水货，返修货等不良备件。

对设备进行日常维护时，投标方应遵循招标方的时间安排。日常维护工作结束后需马上提交问题原因及解决报告。

（3）定期巡检服务

巡检服务必须在现场进行，标书中必须提供巡检项目记录表。巡检结束后当场提交巡检记录表，由巡检人员和招标单位指定人员签字。

2、服务响应及服务人员

要求提供 7×24 小时服务，电话响应在 15 分钟以内，电话支持无法解决问题的情况下 1 小时内到达现场。维护完成后当场提交服务报告，由服务人员和招标方指定人员签字确认。对已发现存在故障需要更换的部件，一般情况应在备件部件到位后 12 小时内完成，当场提交部件设备更换单，并载明原部件型号及序列号、更换部件型号及序列号等内容。

（五）网络设备

1、维保服务内容

包含设备的检测、维护、维修、搬迁，硬件产品固件升级、软件产品版本升级、特征库升级，以及安全策略调整、系统优化、软硬件配置调整等。

更换备件部件费用由投标单位承担，所供备件需为原厂，不得提供假货，水货，返修货等不良备件。

对设备进行日常维护时，投标方应遵循招标方的时间安排。日常维护工作结束后需马上提交问题原因及解决报告。

2、服务响应及服务人员

要求提供 7×24 小时服务，电话响应在 15 分钟以内，电话支持无法解决问题的情况下 1 小时内到达现场。维护完成后当场提交服务报告，由服务人员和招标方指定人员签字确认。对已发现存在故障需要更换的部件，一般情况应在备件部件到位后 12 小时内完成，当场提交部件设备更换单，并载明原部件型号及序列号、更换部件型号及序列号等内容，由服务人员和招标方指定人员签字确认。

若故障影响重要业务运行且无法在 12 小时内修复的，中标方需在 12 小时内提供应急的备机备件保证业务正常运作。

日常维护必须指定至少 1 名或以上固定技术人员，技术人员需具备工信部网络工程师证

书，固定人员在服务期间不得随意更换，如若更换需具备同等资格证书及技术水平，并取得招标单位同意。

（六）安全运维服务要求

1、信息系统安全服务对象

服务对象是宁波市公路与运输管理中心网络安全运维服务，主要包括交通专网、政务外网和市政务云相关信息系统，应对主要信息系统进行定期安全巡检和维护，及时处理系统安全隐患。

2、驻场服务人员要求：

（1）本次安全服务需一位驻场人员，负责信息系统安全运维。要求具有中国信息安全测评中心认证的注册信息安全专业人员工程师证书及工信部网络工程师证书

工作模式：软件辅助与人工巡查相结合；

运维报告：每周提供信息安全运维周报，每月综合性的月报，半年报和全年信息安全运维总结报告等。

3、服务目标及内容综述

（1）服务目标：保证公路运输中心信息系统整体安全稳定运行及满足公安部信息安全等级保护 2 级要求和政府信息系统安全检查要求。

（2）提供对机房和设备运行状况检查，处理各类网络病毒或木马事件；

（3）建立宁波市公路运输中心系统物理设备（包括网络设备、安全设备、服务器设备、终端、存储备份设备、软件安装媒介）档案；

（4）提供宁波市公路运输中心信息系统的安全状况监测、漏洞扫描、安全加固等信息安全运维服务，按要求进行病毒查杀和日志检查，安全审计和日志分析、病毒日志分析、病毒和漏洞公告，确保网络的安全平稳运行；

（5）针对漏洞扫描中出现的安全隐患、对中心现有网络环境的安全风险进行综合分析评估，并制定对应措施和应急方案；配合宁波市公路运输中心进行等保测评工作。

（6）负责制定宁波市公路运输中心业务网应急响应预案，并在应急事件发生时按照预案进行事件处理，保护关键业务免受重大故障或灾难的影响；

（7）为宁波市公路运输中心软硬件平台建设提供安全咨询及服务；

（8）提供宁波市公路运输中心安全方面的不同层次的知识培训，增强信息安全意识。

（9）提供 7*24 小时网站安全服务，保障网站业务的连续性，对出现问题及时解决。

4、服务方式与内容：

（1）日常设备安全监控运维服务

网络设备安全维护：网络设备的日常安全监控，监控重要运行信息，网络链路的连通状态，发现问题及时向公路运输中心安全管理人汇报并协助处理各类网络设备故障和骨干网络链路故障。定期对网络设备监控记录和日志进行分析，发现系统存在的故障隐患和安全隐患，

并提出解决建议。

安全设备维护：检测安全设备工作状态和工作性能，及时升级系统软件，并记录备案，及时处理各类安全设备故障。实时监控各项数据和敏感信息，及时发现问题和安全隐患，并做出相应处理，保障网络通讯安全。对安全设备的参数和配置进行动态的管理，维护配置文档和管理文档，并定期备案。

服务器设备安全维护：监控服务器系统运行情况，查看重要系统参数，并做好记录；维护系统注册表，检查操作系统补丁状况，协助安装操作系统补丁，处理各类操作系统使用问题，监控记录和系统相关日志进行分析，及时发现安全漏洞和安全隐患，及时处理各类服务器软硬件故障。动态管理服务器配置文档，并及时更新发生变化的配置项。定期对服务器维护数据进行统计、分析，并提供设备配置、升级建议。

安全评估及新系统上线评估：服务方需参照 GB/T 20984-2007《信息安全技术 信息安全风险评估规范》国家标准，每年进行一次安全风险评估，通过资产评估、脆弱性评估和威胁评估对现有信息系统和网络可能存在的安全风险进行综合分析评估，并提供相应的风险处置建议；同时，要求服务方对宁波市公路运输中心新上线系统提供评估，保证新系统安全，要求输出评估报告。

基线维护及安全加固：服务方需分析客户信息系统的安全需求，结合本行业等级保护基本要求，建立信息系统安全基线，并在服务期内提供维护管理；同时根据安全基线要求提出详细的安全加固建议，制定严谨的加固实施方案，详细记录判断依据、实施步骤、测试与回退方案等内容，确保加固过程安全、有效，且风险可控。

（2）系统安全巡检

主机漏洞扫描：每季度一次对服务器进行漏洞扫描，掌握服务器的安全状况，要求服务方提供主机漏洞扫描报告。

设备健康巡检：每季度一次对设备进行健康检查，对设备进行配置备份，当发现异常情况时，及时进行跟踪处理。

日志安全审计：每季度一次对设备的防护日志进行审计分析，发现系统威胁来源及威胁类型，及时调整安全防护策略以达到安全防护的目的。

（3）应急响应和应急保障

响应支持级别：服务方针对网络和信息系统突发的重大故障和安全事件提供 7*24 小时的服务，30 分钟赶到现场进行故障排查定位，全力恢复网络和系统正常工作，同时查明故障或入侵来源、时间，并提供应急处置报告。

预案维护：根据宁波市公路运输中心提供的信息系统实际情况，结合当前网络环境及政策法规要求，适时修订应急预案。

应急演练：每年一次协助宁波市公路运输中心对信息系统进行相关的应急模拟演练，并对演练中发现的问题进行总结，演练结束后根据发现的问题进行预案的改进。

（4）不定期安全服务

安全咨询服务：为宁波市公路运输中心网络软硬件平台建设提供信息系统相关安全咨询服务。

系统集成咨询服务：为宁波市公路运输中心评估现有及将来的信息化要求，提出切合实际应用的规划书，并为宁波市公路运输中心的信息化信息安全建设提供建议。可应客户要求，对于新上线的系统，进行信息安全测试，并形成报告书。

安全通告服务：总结最新的安全漏洞信息、黑客攻击方法、流行病毒信息、补丁信息、安全发展动态、浙江省内重大安全事件、安全法律法规等安全资讯，以邮件的方式发送给用户，帮助用户集中了解最新的安全动态。根据事件原因及攻击方法，对网站调整提出专业意见。

（5）专项安全检查

每半年一次协助宁波市公路运输中心对区县公路系统进行检查，协助制订检查方案，安排技术人员到场进行检查支持。检查完成后形成综合分析报告，并针对检查中发现的风险提供整改建议方案以及协助完成整改工作。

每半年一次对宁波市公路运输中心区县公路可互联网访问的信息系统进行应用安全检测，服务方需提供检测分析报告，并协助各单位进行漏洞修复、验证。

在每轮检查完成后，服务方需为宁波市公路运输中心提供检查总结培训，培训内容包含但不限于信息安全意识、信息安全技术、国际和国家层面安全态势等。

（6）统一威胁探针

类别	参数	功能及技术描述
威胁检测	流量采集	支持导入 HTTPS 证书，对流量进行解密和还原。
		支持常见应用的识别不低于 3000 种
		支持流量白名单，过滤掉不关注资产流量，白名单类型应包括 IP、端口、邮箱、域名。
	入侵检测	应覆盖多种攻击特征，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测，攻击特征库数量至少为 8000 种以上。
	扫描检测	支持自定义 TCP/UDP 端口扫描检测模型，结合模型对流量进行检测和告警。
		支持自定义 TCP 端口扫描检测模型，支持配置参数包括检测阈值、检测周期、复位时间，提供默认配置。检测产生的告警信息至少包括扫描类型和扫描事件名称。
		支持自定义 UDP 端口扫描检测模型，支持配置参数包括检测阈值、检测周期、复位时间，提供默认配置。检测产生的告警信息至少包括扫描类型和扫描事件名称。
		内置 WEB 应用机器学习检测模型，支持对 sqli，xss，exec，phprce，ptravel 和 jeli 攻击类型进行分类检测和告警，告警信息至少包括机器学习告警类型和威胁事件名称。
	WEB 应用检测	WEB 类告警详情中包含请求和响应信息，在请求和响应信息中能标记规则匹配中的字段信息，便于运维人员快速进行确认攻击事件。

		支持 WEB 类的攻击结果进行判定
	恶意文件检测	内置恶意文件检测引擎，支持对可执行文件、文档、压缩包和网页脚本进行恶意代码检测和告警，告警信息中至少包含恶意文件类型、恶意文件家族信息和恶意文件变种信息。
	威胁情报检测	支持与威胁情报联动，可进行实时流量匹配检测和告警，支持对恶意 IP、恶意域名、恶意 URL 和恶意文件进行检测。
	WEBshell 检测	内置基于统计学特征和操作码序列训练的检测模型，支持对 asp、jsp、php 文件类型进行检测和告警 内置基于 webshell 通信特点以及流量特征构建决策模型，支持对 asp 文件、php 文件、jsp 文件和图片马进行检测和告警 告警信息至少包括机器学习告警类型和威胁事件名称
	异常行为检测	支持自定义 TCP/UDP 行为检测模型，通过自定义内部资产对流量中的异常行为（包括内部向外部发起、内部对内部发起）进行检测和告警，告警信息包含检测类型和威胁事件名称。
		支持自定义 TCP 行为模型，配置参数至少包括检测阈值、检测周期、复位时间、IP 对象。
		支持自定义 UDP 行为模型，配置参数至少包括检测阈值、检测周期、复位时间、IP 对象。
威胁展示		支持展示威胁告警信息，展示的告警分类包括入侵检测告警、WEB 应用告警、恶意文件告警、威胁情报告警。
	入侵检测告警	入侵检测告警字段至少包括：告警时间、攻击 IP、攻击端口、受害 IP、受害端口、告警类型、事件名称、威胁等级、详情。
	WEB 应用告警	WEB 应用告警字段至少包括：告警时间、攻击 IP、攻击端口、受害 IP、受害端口、告警类型、事件名称、URI、威胁等级、详情。
	恶意文件告警	恶意文件告警字段至少包括：告警时间、攻击 IP、攻击端口、受害 IP、受害端口、传输协议、应用层协议、文件类型、文件名、文件 md5、详情。
	威胁情报告警	威胁情报告警字段至少包括：告警时间、攻击 IP、攻击端口、受害 IP、受害端口、告警类型、事件名称、命中的威胁情报、详情。
回溯分析		应具备元数据提取、存储和检索的能力。
		支持元数据存储和展示，元数据类型至少包括 TCP&UDP 日志、HTTP 日志、EMAIL 日志、FTP 日志、DNS 日志、ICMP 日志、文件还原日志。
响应		支持对入侵检测告警、WEB 应用告警、威胁情报告警和恶意文件告警中的攻击 IP 和受害 IP 发送阻断报文，进行旁路阻断。
		支持自定义一键封堵，配置策略包括 IP 类型（配置选项包括源 ip/源端口/目的 ip/ 目的端口）、域名类型、生效时间和失效时间。
		支持与大数据平台联动：提供 API 接口，由大数据平台通过接口下发一键封堵断策略，探针执行封堵动作并将封堵日志信息发送给大数据平台。
取证（流		支持对采集的全部流量进行存储、检索和下载，检索条件包括源 IP、目的 IP、源端口、目的端口、起止时间。

量存储）		支持自定义规则抓取和留存可疑原始流量，自定义规则支持对原始流量的 payload 进行匹配。自定义规则内容至少包括：源 IP/源端口、目的 IP/目的端口、匹配类型（二进制、字符串、正则表达式）、匹配特征、会话数量、过期时间。
资产识别		支持从流量中识别资产信息和展示，识别的信息至少包括资产 IP、资产 MAC、服务端口号、服务协议、设备类型、地理位置、操作系统、资产状态、资产描述、资产关联账号。
系统管理	备份	支持配置策略的备份，备份数据至少包括全部配置、引擎参数、接口参数和白名单。
		支持备份策略恢复，恢复的类型包括全部配置、引擎参数配置，接口参数配置和白名单配置。
	二次开发	具备二次开发能力，支持第三方通过探针的标准接口进行新的业务开发。
部署能力	部署模式	系统应支持监听（Monitor），能够快速部署在各种网络环境中。
	网络适应能力	系统支持旁路部署，支持 IPv4/IPv6 环境部署。
		系统应支持 VLAN 802.1Q、BGP、MPLS、QinQ、PPPOE 等封装协议，能够适应多种不同的网络环境。

（7）安全威胁监控及响应服务

序号	服务名称	服务数量	说明
1	威胁监控与分析服务	1 年	搭建专业的监控分析平台； 提供 7*24 小时全天候的威胁监控与分析服务；及时对互联网区业务上的威胁事件作出应急响应； 提供专家服务，对热点事件进行预警与防护，对高危访问源进行监控与封杀，对可疑安全事件进行发现与确认。
2	应急响应及技术支持服务	1 年	对突发的安全事件进行响应； 提供应急响应服务，第一事件提供现场应急响应服务和远程技术支持服务； 重保时期，提供现场 7×24 小时的保障服务； 及时提供最新漏洞的检查方式、加固建议等。
3	专业的监控分析平台	1 年	一年租赁费用（整体平台及设备需部署在用户内网）

服务要求

采取人工监控和工具分析相结合的方式对招标方开展 7*24 小时威胁监控与分析工作；监控工程师必须是投标方工程师，需提供社保证明；熟悉招标方现有的网络安全平台，能熟练使用招标方指定的关键网络安全设备，对设备产生的日志告警事件进行分析，并及时作出处置。

服务内容

以招标方现有互联网域的网络安全防护体系为基础，在本地安装部署专业分析工具，搭建专业的监控分析平台，配置合适的威胁监测及分析的模板。

监控分析平台至少包括智能安全运营平台、统一威胁分析系统、漏洞扫描系统等软件、硬件设备，须实现如下功能：

平台功能	功能要求
智能安全	平台支持分布式部署，同时支持软件、硬件的形式部署；能够与监控平台中的

运营平台	统一威胁分析、漏洞扫描、代码审计等系统进行联动，对招标方的数据进行采集、分析、处置。 支持多种协议数据的接入，默认内置至少 300 种各厂商设备日志类型的解析规范化规则，支持招标方现有安全设备的数据接入。 支持资产风险识别，能够实现资产的多维度管理，系统至少内置五种视图：资产组视图、业务系统视图、组织结构视图、地理位置视图、行业视图。 支持漏洞监测分析，能够联动漏洞扫描系统，针对操作系统、业务等自动下发漏动扫描任务，对结果进行展示、分析、建议。 支持日志威胁检测分析，内置不少于 200 种内置分析规则并支持规则库的升级，对可疑安全事件能够按业务系统、网站、终端三种视角进行威胁分析以攻击链阶段统计和展示。 支持对流量日志的分析，发现其中的可疑行为，内含不少于 25 种内置可疑行为分析场景，可疑分析场景包括但不限于：风险账号、内部访问异常、数据泄露等，内置场景支持升级；支持流量数据的查询分析能力，提供会话日志和相关协议日志的关联分析。 平台能结合招标方现有的安全设备，进行全面、综合地分析，主动发现网络中可能存在的安全威胁和安全隐患，评估并展示安全治理等；及时对安全威胁事件作出判断、告警、溯源分析，并提供一键封堵、一键解封等功能的自动处置功能。
统一威胁分析系统	以硬件设备形式接入，要求设备性能满足内存>=32G，硬盘>=4T，吞吐量>=9.8G，最大并发 TCP 会话数>=280 万，每秒新增 TCP 会话数>=60000。 系统支持导入 HTTPS 证书，对流量进行解密和还原；能够针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量、TCP/UDP 的异常行为进行检测，攻击特征库数量至少为 8000 种以上，并对威胁异常行为进行回溯取证分析。 系统支持入侵检测、扫描检测、web 应用检测、恶意文件检查、威胁情报检测、webshell 检测、异常行为检测，并对检测结果进行分析，将威胁告警信息进行分类展示。 系统支持资产的识别，识别的信息至少包括括资产 IP、资产 MAC、服务端口号、服务协议、设备类型、地理位置、操作系统、资产状态、资产描述、资产关联账号。 系统支持溯取证分析，能对采集的全部流量进行存储、检索和下载。
漏洞扫描系统	支持资产的识别和分析，能够对资产进行分级分类管理。 支持检测的漏洞数大于 120000 条，兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准；支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息； 支持扫描大数据组件框架的漏洞，需覆盖 Ambari、Cassandra、Elasticsearch、Flume、Hadoop、Hbase、Hdfs、Hive、 Impala、Kafka、Mongodb、Oozie、Redis、Spark、Storm、Yarn、Zookeeper，要求能够扫描大于 200 条相关漏洞； 支持扫描国产操作系统、应用及软件的安全漏洞，如红旗、麒麟、起点操作系统。 支持扫描主流云主机机管理系统的安全漏洞，如：VMWareESX/ESXi、KVM、Xen，要求能够扫描大于 4000 条相关漏洞。 支持专门针对已有攻击利用代码的漏洞检测，检测用户资产是否存在可利用的漏洞。

①提供 7*24 小时威胁监控、分析服务，对专业工具、网络设备 WAF、IPS 等设备的安全告警进行分析、处置；根据威胁分析结果及时对安全设备策略进行优化，对高危访问源进行监测、封杀；每日提供一份当日监控运维报告（周一至周五，前一天 18:00-当日 9：00；周末全天）。

②针对攻陷类事件进行通告，并对事件的处置情况进行追踪，定期对事件统计分析并反馈事件的处置结果，每周一次。

③提供专家服务，对安全威胁及事故进行调查取证，并提供处置建议。实现热点事件的预警与防护、高危访问源的监测与辅助封杀处置、可疑安全事件的发现与确认。每周至少一次。具体提供的服务内容：

工作内容	工作要求
热点事件的预警与防护	出现热点事件时，及时通过电话、短信、邮件等方式向，将安全事件相关背景信息、漏洞与攻击相关特征及通用处置建议发送给招标方；可在招标方授权下，对安全检测和防护类设备的规则库进行升级并配置安全防护策略。
高危访问源的监测与封杀	利用监控平台及招标方的各类安全设备，及时发现潜在的攻击者，在攻击者找到攻陷方法或路径之前，针对访问源进行拦截。
可疑安全事件的发现与确认	采用互联网边界访问行为检测与流量深度分析相结合的方式，通过系统攻击检测、web 攻击检测、网站安全监测（或通告）和威胁情报等方式，帮助发现并确认可疑的安全事件；快速对可疑事件进行排查和确认，在排查确认后快速向招标方发起安全事件通告，并开始启动应急响应。

（七）机房设备

1、维保服务内容

（1）包扩精密空调、UPS、环境监控、配电等机房设备的检测、维护、维修、清洁、防护、搬迁等。

（2）更换备件部件费用由投标单位承担，所供备件需为原厂，不得提供假货，水货，返修货等不良备件。

（3）每年提供两次精密空调外机清洗服务，及空调过滤网更换服务。

（4）对设备进行日常维护时，投标方应遵循招标方的时间安排。日常维护工作结束后需马上提交问题原因及解决报告。

2、服务响应及服务人员

服务响应为 7×24 小时，电话响应时间 15 分钟，电话支持无法解决问题的情况下现场到达时间为 1 小时，一般故障修复时间为 4 小时，重大故障须与招标单位协商，尽快解决。

（八）桌面设备

1、维保服务内容

（1）包含计算机及打印机等设备的检测、维护、维修、清洁、防护、搬迁等。

（2）对设备进行日常维护时，投标方应遵循招标方的时间安排。日常维护工作结束后需马上提交问题原因及解决报告。

2、服务响应及服务人员

服务响应为 7×24 小时，电话响应时间 15 分钟，电话支持无法解决问题的情况下现场到达时间为 1 小时，一般故障修复时间为 4 小时，重大故障须与招标单位协商，尽快解决。

（九）高速公路视频资源整合平台

1、维保服务内容

（1）包含设备的检测、维护、维修、清洁、防护、搬迁等。

（2）更换备件部件费用由投标单位承担，所供备件需为原厂，不得提供假货，水货，返修货等不良备件。

（3）对设备进行日常维护时，投标方应遵循招标方的时间安排。日常维护工作结束后需马上提交问题原因及解决报告。

（4）维护地点为：宁波市境内高速公路 7 家业务单位 10 个监控中心，具体位置如下：

序号	高速公路业主	监控中心所在地
1	宁波北仑港高速有限公司	甬台温宁波东出口
2	浙江宁波甬台温高速公路有限公司	宁海桑洲（桑洲岭隧道管理所）
3	宁波剡界岭高速公路有限公司	甬金溪口东出口
4	宁波海运明州高速公路有限公司	绕城宁波西出口/甬金宁波西进口
5	宁波市杭州湾大桥发展有限公司	杭州湾大桥庵东出口下去
6	浙江沪杭甬高速公路股份有限公司	杭甬段塘出口
7	宁波交投营运服务有限公司	绕城宁波北出口
8		绕城东东钱湖监控中心(绕城东钱湖出口）
9		象山港大桥咸祥出口
10		穿好高速柴桥出口监控中心大院

2、服务响应及服务人员

服务响应为 7×24 小时，电话响应时间 15 分钟，电话支持无法解决问题的情况下现场到达时间为 1 小时，一般故障修复时间为 4 小时，重大故障须与招标单位协商，尽快解决。

（十）需充放电设备维护

1、维保服务内容

（1）包含充放电设备设备的检测、维护、维修、清洁、防护等。

（2）需提供充放电设备的锂电池更换服务。

（3）对设备进行日常维护时，投标方应遵循招标方的时间安排。日常维护工作结束后需马上提交问题原因及解决报告。

2、服务响应及服务人员

服务响应为 7×24 小时，电话响应时间 15 分钟，电话支持无法解决问题的情况下现场到达时间为 1 小时，一般故障修复时间为 4 小时，重大故障须与招标单位协商，尽快解决。

（十一）路网中心 GQY 大屏延保服务

宁波市公路运输中心路网调度大屏设备主要包括大屏幕投影模块、分布式多屏拼接控制器、高分应用平台及连接线缆等设备组成，是数字公路的基础设施。为确保路网中心数字公

路系统的安全稳定运行，要求有专业资质的供应商对上述设备提供保修和维护。

1、服务数量

（1）设备清单

货物设备名称	规格型号	数量	投运年份	品牌
72 英寸高亮 LED 光源投影机	DDW-E1	32	2015	GQY
玻璃屏幕板	72 英寸	32	2015	GQY
分布式多屏拼接控制器	GQY IPW-D100 （4 路 VGA 输入、8 路 DVI 输入、12 路 HDMI 输入、32 路高清视频输入、4 路 4K 输入、32 路 DVI 输出、含高清底图服务器）	1	2015	GQY
控制软件	GQY 亮度自适应控制模块、无线遥控模块及色彩平衡调节软件；DispManage 拼接屏系统管理软件、DispLink 网络高分辨率传输软件	1	2015	GQY
高分应用平台（含多媒体接入、交通综合管理可视化信息）	含超高分辨率 GIS 电子地图快速显示模块、视频监控模块。	1	2015	GQY
72 英寸箱体套件	72 寸反射机箱	32	2015	GQY
底架		8	2015	GQY

2、服务范围

服务对象是宁波市公路路网中心调度大屏设备,主要包括大屏幕投影模块、分布式多屏拼接控制器、高分应用平台及连接线缆等，供应商应对清单中设备进行定期巡检和维护，及时处理设备故障（免费更换和维修故障配件或设备）

3、总体要求

供应商应在充分理解招标文件的基础上，提供完整的投标维保方案，投标维保方案应包括但不限于以下内容：供应商对项目管理及质量控制，检测设备、服务人员组成等。

4、服务内容

（1）大修改造

如设备损坏，须根据所购配件对大屏幕投影模块和图像处理模块进行更换调试，达到产品设计验收要求，按《视频显示系统工程技术规范》（GB50464-2008）标准，采用实地方式验收，由甲方出具服务项目验收证明。

（2）现场保障

在所提供技术服务期限内服务期内派驻现场专职技术人员 1 名提供技术保障及运维服务；

在所提供技术服务期限内应配合用户完成中心相关设备安装、搬运及机房布线等安装、搬运及技术服务工作。

（3）预防性现场巡检维护保养保障

供应商应对服务范围内的系统做定期的现场巡检和维护保养，周期为每月一次，对维保

设备的整体运行状态进行评估分析，填写设备巡检报告。重点在于硬件设备及与之相关的各种环境信息、状态的检查，并根据检查结果提供建议，必要时进行预防性维修。逢重大节假日或保供电前期按采购人要求做特殊巡检和维护保养。维护保养的内容至少包括：

投影模块

屏幕清洁；机芯维护；镜头维护；电源模块检查；箱体全面除尘清尘；灯组的检查和清洁；检查投影模块和图像控制器的工作是否正常。

控制器和控制终端

控制器开箱检查；控制器的清洁；控制器硬、软件检测，部件更换；操作控制软件的升级服务和质保服务；控制器和控制终端病毒清理。

投影系统

线缆检查；视频检查；网络检查；投影显示亮度综合检查；系统色彩平衡一致性调整；系统显示图像位置调整，投影模块几何线性调整；检查大屏幕系统的各路信号源使用是否正常；调试大屏幕机械位置和颜色色差；查看大屏幕系统的使用环境；测试易损耗配件的使用情况。

（4）供应商应在投标文件中制定相应的定期维保计划，并按照维保计划及时到采购人现场进行维护保养。

（5）每次定期维护保养结束，供应商应及时提供维护保养报告，详细记录系统诊断过程、操作步骤、必要的系统优化调整建议等。

（6）故障维护

当服务范围内的系统及设备出现故障并向供应商报修时，供应商服务人员应按要求，携带相关检测仪器、备件和材料及时抵达现场进行诊断并排除硬件故障，使系统恢复正常运行，未经许可，供应商不得借助采购人的任何资源。

供应商进行故障排查时，不得发生因对设备的操作导致其他无关设备的异常和故障，或系统故障的进一步扩大。

采购人在使用服务范围内的设备时如遇到问题，随时可以从供应商立刻得到电话支持与帮助。

对于通过电话无法解决的问题，要求供应商服务人员在规定的时间内到达现场服务。如果在现场服务中，由于供应商的技术人员的误操作而导致采购人的系统运行受到影响，供应商将承担全部责任。

所有服务范围内的设备出现硬件故障，供应商均应免费修复或者更换。替换的零部件应按硬件厂商的更换规则进行了必要的升级，以优化用户的系统性能。更换零部件的保修期及保修级别与主设备一致。

每次故障维护结束，供应商应及时提供故障维护报告，详细记录处理过程和结果等，内容包括服务请求、开始时间、结束时间、电话支持内容、现场工作纪要、备件更换情况、故

障现象、故障处理方式以及处理结果、设备运行状况等。

采购人系统出现运行问题时，原因可能是多方面的，如操作系统问题、硬件问题、应用软件问题、数据库问题等，基于此原因，供应商应制定多厂家协作支持服务方案，协助采购人迅速诊断，综合解决问题。

（7）整体调优

供应商在做好设备维保工作的同时，应做好系统的整体调优工作，使得系统处于可靠、安全的运行方式，显示画面亮度、色彩和对比度整体均匀，并具有较高的运行效率。供应商负责将设备厂商最新发现的重要问题与 Bug 及时通知采购人，在征得采购人同意后采取相应的防范措施。

（8）故障应急

供应商应在合同生效后一个月内提供设备的应急方案，做好配置文件备份和其它相应的事故预想工作。

（9）培训

供应商应在故障维护的同时，针对性地对故障的现象、分析、诊断、定位等向采购人进行现场指导培训。

（10）服务要求

基本要求

服务期间应遵守采购人的安全制度、保密制度、运维规程，签订保密协议，保证不发生安全事故、泄密事件。

未经采购人同意，供应商不得随意变更服务人员，以及安排常驻服务人员与采购人无关的其它工作。

提供 7×24 小时电话支持，随时接受采购人的技术咨询，帮助采购人迅速解决较容易的、非现场的技术问题。

故障响应要求：在设备故障时，供应商应承诺 7*24 小时服务，在接到故障报修请求后 60 分钟内到达现场，开展故障检测、定位、排除工作（含损坏件更换）。

故障恢复要求：常规的单点或多点故障，在供应商接到故障报修请求后，应于 4 小时内排除故障，恢复正常。特殊故障，如同一故障反复频繁出现等情况，则由供应商制定完整的解决方案，并经过采购人技术负责人确认后，由采购人技术负责人安排合适的时间，通过分阶段排查解决。

供应商服务人员在现场实施过程中所使用的检测设备等应是安全可靠的专用设备，专用笔记本计算机设备应根据维保设备类型预装相应检测软件，放置在采购人现场统一管理。

在服务期结束时，提交运维服务工作总结报告。

维护的主要材料和所需的消耗性材料均由供应商免费提供，且必须为采购人储备充足的易损耗配件，确保采购人大屏幕系统的常年正常运行，并每月对大屏幕机体内外进行清洁工

作。

在维保过程中，供应商如果通过维保或者自行检查，发现大屏幕系统仅依靠合同规定的维保已经不能保证安全运行，需要改造、维修或者更换零部件、更新设备时，应当向采购人书面提出，并进行免费改造、维修或者更换零部件、更新设备；发现事故隐患及时告知甲方。

调试维护必须保证质量，确保设备维护后一年内不发生因维护原因造成的设备事故。否则，供应商应当无条件免费返修，返修质量达到符合采购人要求为止。

（11）人员要求

供应商需指定一名主要联系人及两名替补联系人与采购人联系。

供应商指定的现场服务人员应具有专业资质，应将现场服务人员的简历（学历、工作经历）、项目经历（需用户证明）、技能情况、资格证明等在现场备案。

（12）工作要求

建立和完善例行运维手册，根据系统运行状况，建立必要的系统运维监控文档，包括运维规程、运维任务清单、典型运维操作手册等。

建立配置文档，描述系统的组成和结构，建立各系统配置清单，根据系统变更情况及时更新调整系统配置清单。

系统变更维护，根据应用需要，及时调整系统的应用软件及相关技术配置，使系统功能能够满足应用需求，使系统能够保持正常运行。

（十二）其他要求

1、文档管理

投标方需提供本次维保涉及的各类文档、表格，包括但不限于：巡检项目记录表，日常服务报告\故障处理单和部件设备更换单。

2、运维管理

投标方需协助招标单位建立、完善设备运维管理制度及文档，包括但不限于：相关设备的运维操作规程，相关设备及配套软件的日常维护操作文档和故障应急处置方案。同时，要求每季度提交机房运维总体报告，内容包括此季度维保响应次数、时间、人员、内容，备件储备及使用情况，设备健康情况，运维建议等。

3、备品备件

为确保宁波公路运输中心核心机房信息化设备的正常运行，中标单位必须提供备品备件服务，在服务期限内备品备件必须放置在用户处。备件具体要求如下：

备品备件清单

备件类型	备件名称	配置要求	数量	存放地点	品牌要求
网络安全设备	防火墙	百兆防火墙	1	用户机房	国产主流
	安全审计设备	日志审计设备	1	用户机房	国产主流

	核心交换机	双引擎，配置 24 口千兆电口业务板 2 块，配 48 口千兆电口业务板 1 块，12 口以上千兆 sfp 光口业务板 1 块。	1	用户机房	CISCO/H3C/华为
	交换机	24 口可网管交换机	2	用户机房	CISCO/H3C/华为
	多模模块	万兆 SFP 多模模块	4	用户机房	CISCO/H3C/华为
	单模模块	光模块-SFP-GE-单模模块，1310nm，10KM	4	用户机房	CISCO/H3C/华为
服务器	硬盘	300G SAS 3.5 寸 15K	2	用户机房	联想/HP/DELL
	硬盘	3TB SAS 2.5 寸	2	用户机房	联想/HP/DELL
	电池	495W 电池	2	用户机房	联想/HP/DELL
	电源	750W 电源	2	机房	联想/HP/DELL
存储	硬盘	3.5 寸 600G 15K 存储专用硬盘	4	机房	EMC（vnx 系列）

四、*商务要求

序号	内　　容
1	合同签订时间：中标通知书发出后 30 天内。
2	服务地点：采购人指定地点。
3	服务期限：一年。
4	付款方式： 合同签订并具备实施条件后 7 个工作日内，采购人支付合同款的 40%作为预付款；剩余 60%在服务期满后根据考核结果一次性付清。 注：在签订合同时，中标人明确表示无需预付款或者主动要求降低预付款比例的，以中标人意愿为准。
5	履约保证金：无。
6	质量及验收标准： 质量及验收标准必须执行国家相关标准、行业标准、地方标准或者其它标准、规范（从严）：具有国家标准及规范的，按最新的标准及规范执行；具有行业标准及规范的，按最新的标准及规范执行；具有其他标准及规范的，按照最新的标准及规范执行；符合招标文件的实质性技术要求。
7	考核： 每月针对服务满意度进行打分（详见**附件一：服务满意度月度评分表**），考核总分为100分。每月分数不低于90分的，合同尾款全额支付；月分数低于90分的，每低1分，扣除1万，最多扣除12万元。服务期内累计3个月考核低于90分的，采购人有权解除合同。
8	合同终止： 中标人在合同有效期内，不得以任何理由终止合同，确有特殊情况的，须提前两个月向采购人提出书面申请，经采购人同意后，方可终止合同。因中标方不能保证工作质量，或发生重大差错事故的，采购人有权终止协议，供应商承担全部责任。
9	其他： 在采购及合同执行过程中，供应商应承担由于其行为所造成的人身伤害、财产损失或损坏的责任，无论何种原因所造成，采购人均不负责。

附件一：服务满意度月度评分表

服务满意度月度评分表						
姓名		考评时间		考评人		
考核内容	考核标准	考核计分说明		分值	得分	备注
日常工作	是否及时响应客户需求	满意 5 一般 4 不满意 3		5		
	服务态度是否端正	满意 5 一般 4 不满意 3		5		
	是否及时完成工作	满意 5 一般 4 不满意 3		5		
应急处理	数据备份情况，制定备份策略并定期进行备份检查	满意 10 一般 9 不满意 8		10		
	发生信息化事件后作相关记录，进行报告，并采取积极合理的措施进行处置	满意 10 一般 9 不满意 8		10		
环控管理	保证机房温度恒定在 20℃-30℃之间	满意 10 一般 9 不满意 8		10		
	保证 UPS 工作正常，电池无漏液	满意 10 一般 9 不满意 8		10		
设备管理	交换机，路由器等网络设备的正常运行	满意 10 一般 9 不满意 8		10		
	服务器工作是否正常	满意 10 一般 9 不满意 8		10		
	及时更换故障硬盘	满意 10 一般 9 不满意 8		10		
技术支撑	完成领导与其他单位网络对接的任务，配合软件公司部署服务器等工作	满意 15 一般 14 不满意 13		15		
合计				100		

第三章　供应商须知

前附表

序号	内容、要求
1	**项目名称：信息化设备及安全服务外包项目**
*2	**本项目预算金额：**人民币 1268300 元。
*3	**投标报价及费用：** 1、报价方式：**本项目投标应以人民币报价。**供应商须报完成招标内容及要求所提供的服务过程中涉及的所有费用。包括但不限于以下内容：人工费、差旅费、维护费、备品备件费、管理费、利润、风险因素、规费、税金等一切与完成本项目相关的费用。 2、本项目不接受有选择的报价。 3、不论投标结果如何，供应商均应自行承担所有与投标有关的全部费用。
4	**投标保证金：**无。
5	**现场踏勘（如有）：**/。
6	**演示时间及地点（如有）：**/。
7	**本项目实行网上投标，供应商应准备以下投标文件：** （1）上传到政府采购云平台的电子投标文件（资格证明文件、商务技术文件、报价文件）1份。 （2）以U盘存储的电子备份投标文件（资格证明文件、商务技术文件、报价文件）1份。
*8	**投标截止时间及地点：**详见《公开招标采购公告》。
*9	**开标时间及地点：**详见《公开招标采购公告》。
10	**评标办法及评分标准：**详见第四章。
11	**中标结果公告：**评标结束后，评标结果公示网站详见第一章《公开招标公告》，同时向中标供应商发出中标通知书。
12	**投标保证金退还：**无。
13	**签订合同时间：**中标通知书发出之日起30日内签订合同，具体签约时间以采购人通知为准。
*14	**投标文件有效期：** 90 天

15	**招标代理服务费：**本招标公司根据国家发改委发改办价格[2003]857 号通知和国家计委计价格[2002]1980 号文件的规定服务招标费率标准的 65%，按照中标通知书确定的中标金额，向中标人收取招标服务费。
16	**解释：**本采购文件的解释权属于采购单位和招标代理机构。

注：本前附表内打有“*”号的条款为“实质性要求”条款，投标文件对这些条款的任何负偏离将视为没有对采购文件的实质性要求做出响应，将被认定为无效投标。

一、总则

（一）适用范围

本采购文件适用于本采购项目的招标、投标、评标、定标、验收、合同履约、付款等行为（法律、法规另有规定的，从其规定）。

（二）定义

1.“采购人”系指组织本次招标的采购单位（“采购人”）。

2.“投标人”系指向采购人提交投标文件的单位或个人（“供应商”）。

3.“服务”系指采购文件规定投标人须承担的完成与本项目有关的一切服务以及其他类似的义务。

4.“项目”系指投标人按采购文件规定向采购人提供的产品和服务。

5.“书面形式”包括信函、传真、电报等。

6.“*”系指实质性要求条款。

（三）招标方式

本次招标采用公开招标方式进行。

（四）投标委托

如供应商派授权代表出席开标会议，授权代表须携带有效身份证件。投标人代表须为投标人的在职员工，如投标人代表不是法定代表人，须有法定代表人出具的授权委托书并在投标文件中提供投标人代表身份证正反面复印件及授权代表开标之日前三个月内近一个月的投标人所缴纳的社保证明（投标文件正本用原件，副本可用复印件，格式见第六部分）。

（五）投标费用

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

（六）联合体投标

不接受联合体投标。

（七）转包与分包

本项目不允许转包，未经采购人同意，不得分包。

（八）特别说明

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

***2.投标人在投标活动中提供任何虚假材料，其投标无效，并报监管部门查处；中标后发现的,中标人须依照《中华人民共和国消费者权益保护法》第55条之规定赔偿采购人，且民事赔偿并不免除违法投标人的行政与刑事责任。**

（九）关于分公司投标

除银行、保险、石油石化、电力、电信、移动、联通等行业允许分公司投标外，其余不允许分公司投标。如允许分公司投标的，需提供具有法人资格的总公司的营业执照原件扫描件及授权书，授权书须加盖总公司公章。总公司可就本项目或此类项目在一定范围或时间内出具授权书。已由总公司授权的，总公司取得的相关资质证书对分公司有效。

（十）关于知识产权

1.投标人必须保证，采购人在中华人民共和国境内使用投标货物、资料、技术、服务或其任何一部分时，享有不受限制的无偿使用权，如有第三方向采购人提出侵犯其专利权、商标权或其它知识产权的主张，该责任应由投标人承担。

2.投标报价应包含所有应向所有权人支付的专利权、商标权或其它知识产权的一切相关费用。

3.系统软件、通用软件必须是具有在中国境内的合法使用权或版权的正版软件，涉及到第三方提出侵权或知识产权的起诉及支付版税等费用由投标人承担所有责任及费用。

（十一）质疑和投诉

1.供应商认为采购文件、采购过程、中标或者成交结果使自己的权益受到损害的，须在应知其利益受损之日起七个工作日内以书面形式向采购人、采购代理机构提出质疑。供应商应当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。

2.提出质疑的供应商应当是参与所质疑项目采购活动的供应商。未依法获取采购文件的，不得就采购文件提出质疑；未提交投标文件的供应商，视为与采购结果没有利害关系，不得就采购响应截止时间后的采购过程、采购结果提出质疑。

3.供应商提出质疑应当提交质疑函和必要的证明材料，质疑函应当以书面形式（需符合财政部令第94号政府采购质疑和投诉办法要求）提出。

4.接收书面质疑函的方式：质疑人可通过送达、邮寄、传真的形式提交书面质疑函，通过邮寄方式提交的书面质疑函以被质疑人签收邮件之日为收到书面质疑文件之日，通过传真方式提交的书面质疑函以被质疑人收到书面质疑文件原件之日为收到书面质疑文件之日。被质疑人处理质疑联系部门：本采购文件第一章中采购代理机构的有关联系方式。

5.供应商对采购人或采购代理机构的质疑答复不满意或者采购人或采购代理机构未在规定时间内作出答复的，可以在答复期满后十五个工作日内向同级采购监管部门投诉，投诉须采用书面形式（需符合财政部令第94号政府采购质疑和投诉办法要求）。

二、采购文件

（一）采购文件的构成。

本采购文件由以下部分组成：

1.公开招标采购公告

2.采购需求

3.供应商须知

4.评标办法及评分标准

5.政府采购合同主要条款

6.投标文件格式

7.本项目采购文件的澄清、答复、修改、补充的内容

（二）供应商的风险

1、供应商没有按照采购文件要求提供全部资料，或者供应商没有对采购文件在各方面作出实质性响应是供应商的风险，并可能导致其投标被拒绝。

2、采购文件中标注“*”号的为要求供应商作实质性响应的重要商务或技术条款，供应商的投标对任何带“*”号的重要商务或技术条款的偏离或未作实质性响应都将直接导致投标被拒绝或评定为无效投标。

（三）采购文件的澄清与修改

1.采购人可主动地或在解答投标人提出的澄清问题时对采购文件进行必要的澄清或者修改的，在发布招标公告的网站上发布更正公告，更正公告为采购文件的组成部分，一经在网站发布，视同已通知所有采购文件的收受人。澄清或者修改的内容可能影响投标文件编制的，更正公告在投标截止时间至少 15 日前发出；不足 15 日的，顺延提交投标文件截止时间。

2.澄清或者修改的内容可能影响投标文件编制的，采购代理机构将以书面形式通知所有获取采购文件的潜在投标人，并对其具有约束力。投标人在收到上述通知后，应及时向采购代理机构确认。投标人未回复的，视同已知晓澄清或者修改的内容。

因潜在投标人原因或通讯线路故障导致通知逾期送达或无法送达，采购代理机构不因此承担任何责任，有关的招标采购活动可以继续有效进行。

3.如更正公告有重新发布电子采购文件的，投标人应下载最新发布的电子采购文件制作投标文件。

4.投标人在规定的时间内未对采购文件提出疑问、质疑或要求澄清的，将视其为无异议。对采购文件中描述有歧义或前后不一致的地方，评标委员会有权进行评判，但对同一条款的评判应适用于每个投标人。

三、投标文件的编制

供应商应按照采购文件的要求编制投标文件，并对采购文件提出的要求和条件作出实质性响应。

（一）投标文件的组成

投标文件由资格证明部分、商务技术部分、投标报价部分组成。

资格证明文件：

（1）有效的企业法人营业执照（或事业法人登记证）、其他组织（个体工商户）的营业执照或者民办非企业单位登记证书复印件（复印件加盖公章）；

（2）具备履行合同所需的设备和专业技术能力的声明（格式见附件）；

（3）近三年在政府采购活动中无重大违法记录的声明（格式见附件）；

（4）供应商资格声明（格式见附件）；

（5）中小企业声明函：本项目专门面向中小企业采购，供应商应为中小微企业、监狱企业、残疾人福利性单位，供应商需提供《中小企业声明函》（格式见附件）、《残疾人福利性单位声明函》（若有，格式见附件）；

（6）特定的资格要求：无。

商务技术部分：

（1）法定代表人的身份证明或法定代表人授权书【供应商的代表若为非法定代表人的，必须提交法定代表人授权书及授权代表首次开标之日前近三个月供应商所缴纳社保证明（均加盖公章），格式见附件】；

（2）供应商基本情况说明（格式见附件）；

（3）商务条款偏离表(格式见附件）；

（4）技术条款偏离表（格式见附件）；

（5）类似项目业绩表（格式见附件）；

（6）项目负责人简历表（格式见附件）；

（7）项目人员配置表（格式见附件）；

（8）第四章“评分办法及评分标准”中评分标准要求提供的资料；

（9）供应商针对商务技术部分需要说明的其他文件和说明。

报价部分：

（1）投标函（格式见附件）；

（2）开标一览表（格式见附件）；

（3）报价明细表（格式见附件）；

（4）供应商自觉抵制政府采购领域商业贿赂行为承诺书（格式见附件）；

（5）供应商针对报价需要说明的其他文件和说明。

备注：如未提供格式的，投标人可自拟。

（二）投标文件的语言及计量

***1.投标文件以及投标人与采购人就有关投标事宜的所有来往函电，均应以中文汉语书写。除签名、盖章、专用名称等特殊情形外，以中文汉语以外的文字表述的投标文件视同未提供。**

***2.投标计量单位，采购文件已有明确规定的，使用采购文件规定的计量单位；采购文件没有规定的，应采用中华人民共和国法定计量单位（货币单位：人民币元），否则视同未响应。**

（三）投标报价

1.投标报价应按采购文件中相关附表格式填写。

***2.投标文件只允许有一个报价，有选择的或有条件的报价将不予接受。**

（四）投标文件的有效期

***1.自投标截止日起90天投标文件应保持有效。有效期不足的投标文件将被拒绝。**

2.在特殊情况下，采购人可与投标人协商延长投标书的有效期，这种要求和答复均以书面形式进行。

3.投标人可拒绝接受延期要求。同意延长有效期的投标人，不能修改投标文件。

4.中标人的投标文件自开标之日起至合同履行完毕止均应保持有效。

（五）投标文件的盖章、签署、份数、要求及效力

1、供应商应按本采购文件规定的格式和顺序编制、装订投标文件，投标文件要求有目录并标注页码，投标文件内容不完整、编排混乱导致投标文件被误读、漏读或者查找不到相关内容的，是供应商的责任。

2、投标文件的盖章、签署：

电子投标文件及电子备份投标文件中涉及到加盖公章或签字的，加盖供应商公章部分均采用CA签章，签字部分采用电子签章。

3、投标文件的份数：

本项目供应商应准备以下投标文件：

（1）上传到政府采购云平台的电子投标文件（含资格证明文件、商务技术文件、报价文件）1份。

（2）以U盘存储的电子备份投标文件（含资格证明文件、商务技术文件、报价文件）1份。

4、电子投标文件：

4.1供应商应根据“政采云供应商项目采购-电子招投标操作指南”及本采购文件规定的格式和顺序编制电子投标文件并进行关联定位。

5、投标文件的效力：

投标文件的启用，按先后顺位分别为“电子加密投标文件”→“电子备份投标文件”。在下一顺位的投标文件启用时，前一顺位的投标文件自动失效。

（六）投标文件的包装、递交、修改和撤回

1、以U盘存储的电子备份投标文件用封袋密封后递交。

2、未按规定密封或标记的投标文件将被拒绝，由此造成投标文件被误投或提前拆封的风险由供应商承担。

3、供应商在投标截止时间之前，可以对已提交的电子备份投标文件进行修改或撤回，并书面通知招标采购单位；投标截止时间后，供应商不得撤回、修改投标文件。修改后重新

递交的电子备份投标文件应当按本采购文件的要求签署、盖章和密封。

4、供应商应当在投标截止时间前完成电子投标文件的传输递交，并可以补充、修改或者撤回电子投标文件。补充或者修改电子投标文件的，应当先行撤回原文件，补充、修改后重新传输递交。投标截止时间前未完成传输的，视为撤回投标文件。投标、响应截止时间后传输递交的投标、投标文件，将被拒收。

（七）投标无效的情形

实质上没有响应采购文件要求的投标将被视为无效投标。投标人不得通过修正或撤消不合要求的偏离或保留从而使其投标成为实质上响应的投标。投标无效情形详见第四章《评标办法及评分标准》。

四、开标

（一）开标准备

采购代理机构将在规定的时间和地点进行开标，供应商的法定代表人或其授权代表可参加开标会。供应商的法定代表人或其授权代表未参加开标会的，视同放弃开标监督权利、认可开标结果。

（二）开标程序

1、电子招投标开标程序：

第一阶段：

（1）投标截止时间后，供应商登录政府采购云平台，用“项目采购-开标评标”功能对电子投标文件进行在线解密，在线解密电子投标文件时间为开标时间后 30 分钟内。

（2）在政府采购云平台开启已解密供应商的“投标文件”；

第二阶段：

（1）在政府采购云平台宣告第一阶段评审无效供应商名单及理由；

（2）公布经第一阶段评审符合采购文件要求的供应商的商务技术得分和报价得分情况；

（3）在政府采购云平台公布评审结果。

（4）开标会议结束。

2、特别说明：政府采购云平台如对电子化开标及评审程序有调整的，按调整后的程序操作。

本项目原则上采用政采云电子招投标开标程序，但有以下情形之一的，按以下情况处理：

（1）若有供应商在规定时间内无法解密或解密失败，代理机构将开启该供应商递交的以 U 盘存储的电子备份投标文件，上传至政采云平台项目采购模块，以完成开标，电子投标文件自动失效。

（2）若因政府采购云平台原因无法读取或电子开评标无法正常进行，代理机构将开启所有供应商递交的电子备份投标文件，以完成开标。

（3）采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子

交易的公平、公正和安全时，采购人（或代理机构）可中止电子交易活动：

2.1 电子交易平台发生故障而无法登录访问的；

2.2 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；

2.3 电子交易平台发现严重安全漏洞，有潜在泄密危险的；

2.4 病毒发作导致不能进行正常操作的；

2.5 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，采购人（或代理机构）可以待上述情形消除后继续组织电子交易活动，也可以决定某些环节以纸质形式进行。

（4）未开启的备份投标文件现场予以退还。

五、评标

（一）组建评标委员会

本项目评标委员会由采购人代表和评审专家组成或全部由评审专家组成，评审专家从专家库随机抽取。

（二）评标方法

评标方法见第四章。

（三）评标程序

评标程序见第四章

（四）评标过程保密

中标结果公示发布之前，评标委员会名单应该保密。评标委员会成员、采购人和采购代理机构的有关参与人员应该对评标过程保密，不得向投标人或其他无关的人员透露。

六、定标

（一）确定中标人

1.本项目由评标委员会推荐中标候选人，采购人不得在评标委员会推荐的中标候选人以外确定中标候选人。

2.采购代理机构在评标结束后 2 个工作日内将评标报告交采购人确认，采购人在收到评标报告之日起 5 个工作日内在评标报告确定的中标候选人中按顺序确定中标人，采购人在收到评标报告之日起 5 个工作日内未按评标报告推荐的中标候选人排序确定中标人，又不能说明合法理由的，视同按评标报告推荐的顺序确定综合得分第一的中标候选人为中标人。

3.采购代理机构自中标人确定之日起 2 个工作日内，在发布招标公告的网站上对中标结果进行公示，中标结果公告期限为 1 个工作日。

4.凡发现中标人有下列行为之一的，将移交政府采购监督管理部门依法处理：

（1）提供虚假材料谋取中标的；

（2）采取不正当手段诋毁、排挤其他投标人的；

（3）与采购人、其他投标人或者采购代理机构工作人员恶意串通的；

（4）向采购人或采购代理机构人员行贿或者提供其他不正当利益的；

（5）拒绝有关部门监督检查或者提供虚假情况的；

（6）有法律、法规规定的其他损害采购人利益和社会公共利益情形的。

或

1.本项目由采购人事先授权评标委员会直接确定中标人。

2.凡发现中标人有下列行为之一的，将移交政府采购监督管理部门依法处理：

（1）提供虚假材料谋取中标的；

（2）采取不正当手段诋毁、排挤其他投标人的；

（3）与采购人、其他投标人或者采购代理机构工作人员恶意串通的；

（4）向采购人或采购代理机构人员行贿或者提供其他不正当利益的；

（5）拒绝有关部门监督检查或者提供虚假情况的；

（6）有法律、法规规定的其他损害采购人利益和社会公共利益情形的。

七、评标过程的监控

本项目评标过程实行全程录音、录像监控，投标人在评标过程中所进行的试图影响评标结果的不公正活动，可能导致其投标被拒绝。

八、合同授予

（一）签订合同

1.采购人应当自中标通知书发出之日起30日内，按照采购文件和中标人投标文件的规定，与中标人签订书面合同。所签订的合同不得对采购文件确定的事项和中标人投标文件作实质性修改。

采购人不得向中标人提出任何不合理的要求作为签订合同的条件。

2.采购人在签订合同时，在合同金额变更范围内，如需审批的办理相关审批手续。有权变更采购项目的数量和服务内容，但不能对单价或其他条款和条件作任何改变。

3.采购文件、中标供应商的投标文件及评标过程中有关的澄清文件均应作为合同签订的附件。

4.中标或者成交供应商拒绝与采购人签订合同的，采购人应重新招标。

5.中标人如不遵守采购文件或投标文件各项条款的邀约与要约，或在接到中标通知书后借故拖延，拒签合同的，采购人将按《浙江省政府采购供应商注册及诚信管理暂行办法》的规定上报诚信状况。给采购人造成的损失的还应当予以赔偿。

（二）履约保证金

无。

九、特别说明

1.1 本项目为**专门面向中小企业**采购。

1.2 本项目对应的中小企业划分标准所属行业：**其他未列明行业**。

1.3 中小企业是指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。

国务院批准的中小企业划分标准：具体见工信部联企业[2011]300 号。

1.4 采购活动过程中，对供应商的“中小企业”资格认定，以供应商提交的《中小企业声明函》为准，供应商必须实事求是地提交声明函，如有虚假，将依法承担法律责任。如果在采购活动过程中相关采购当事人对供应商“中小企业”资格有异议的，由货物制造商或者工程、服务供应商注册登记所在地的县级以上人民政府中小企业主管部门负责认定。

供应商提供声明函内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。

适用招标投标法的政府采购工程建设项目，投标人提供声明函内容不实的，属于弄虚作假骗取中标，依照《中华人民共和国招标投标法》等国家有关规定追究相应责任。

1.5 按规定享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。

2.根据《财政部司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68 号）规定，监狱企业视同小型、微型企业。监狱企业参加政府采购活动时，应当提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

3.根据《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，在政府采购活动中，残疾人福利性单位视同小型、微型企业。残疾人福利性单位参加政府采购活动时，提供《残疾人福利性单位声明函》。

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

*5.投标人在投标活动中提供任何虚假材料，其投标无效。

第四章　评标办法及评分标准

本办法严格遵照《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《政府采购货物和服务招标投标管理办法》，结合项目所在地政府有关政府采购规定和项目的实际情况制定。

一、评标委员会

（一）本次招标依法组建评标委员会。评标委员会由采购人代表和评审专家组成或全部由评审专家组成，评审专家从专家库随机抽取。

（二）评标原则。评标委员会必须遵循公平、公正、客观、科学的原则和规定的程序进行评标；评标的依据为采购文件和投标文件；评审人员应独立评标，不得带有任何倾向性和启发性影响他人评审；任何单位和个人不得干扰、影响评标的正常进行；评标委员会及有关工作人员不得私下与投标人接触，不得向外界透露任何与评标有关的内容。

（三）评审专家有下列情形之一的，受到邀请应主动提出回避，采购当事人也可以要求该评审专家回避：

1、参加采购活动前三年内，与供应商存在劳动关系，或者担任过供应商的董事、监事，或者是供应商的控股股东或实际控制人；

2、与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

3、曾经参加过本项目的进口产品论证工作；

4、与供应商有其他可能影响政府采购活动公平、公正进行的关系。

（四）评标委员会判断投标文件的有效性、合格性和响应情况，仅依据投标人所递交一切文件的真实表述，不受与本项目无直接关联的外部信息、传言而影响自身的专业判断。

（五）评委依法独立评审，并对评审意见承担个人责任。评委对需要共同认定的事项存在争议的，按照少数服从多数的原则做出结论。持不同意见的评委应当在评审报告上签署不同意见并说明理由，否则视为同意。

二、评标方法

（一）本次招标项目的评标方法为：综合评分法。

（二）评分权重

评分项目	商务技术分（分）	价格分（分）
权重	88	12

1、价格分采用低价优先法计算，即满足采购文件要求且参与评审价格最低为评标基准价，其价格分为满分。其他投标人的价格分按照下列公式计算：

价格分=（评标基准价/投标报价）×价格权值×100

2、合格投标人评标综合得分=商务技术分+价格分。

3、报价要求：本次招标设有预算价(或最高限价），投标人报价超出预算价(或最高限价）的投标文件作无效处理。

4、采用综合评分法的，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。投标文件满足采购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的为第一中标候选人，得分次高的投标人的为第二中标候选人。

（三）投标文件的澄清

1、对于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，评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者补正。

2、投标人的澄清、说明或者补正应当采用书面形式（或扫描件上传政采云平台），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。

（四）投标文件错误修正原则

投标文件报价出现前后不一致的，除采购文件另有规定外，按照下列规定修正：

1.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；

2.大写金额和小写金额不一致的，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；

5.政采云平台填报的开标一览表中的价格与上传的报价文件中开标一览表的报价不一致的，以上传的报价文件为准。

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具有约束力，若投标人不确认的，则其投标无效。

（五）废标情况

评标过程中，出现下列情形之一的，应予废标，评标终止：

1.通过资格审查、符合性审查的投标人不足三家的；

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。

三、评标过程

1.资格审查

依据法律法规和采购文件的规定，采购人或采购代理机构对投标人对投标文件中的资格证明进行审查，以确定投标人是否具备投标资格。

检查内容

（1）有效的企业法人营业执照（或事业法人登记证）、其他组织（个体工商户）的营业执照或者民办非企业单位登记证书复印件（复印件加盖公章）； （2）供应商资格声明（格式见附件）； （3）中小企业声明函：本项目专门面向中小企业采购，供应商应为中小微企业、监狱企业、残疾人福利性单位，供应商需提供《中小企业声明函》（格式见附件）、《残疾人福利性单位声明函》（若有，格式见附件）； （4）特定的资格要求：无。

2.符合性审查

依据采购文件的规定，评标委员会应当对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足采购文件的实质性要求。

序号	评审因素		评审标准
1	有效性审查	投标文件签署	投标文件上法定代表人或其授权代表人的签字齐全。
		法定代表人身份证明及授权委托书	法定代表人身份证明及授权委托书有效，符合采购文件规定的格式，签字或盖章齐全。
		投标方案	每个分包只能有一个方案投标。
		报价唯一	只能在采购预算范围内报价，只能有一个有效报价，不得提交选择性报价。
2	完整性审查	投标文件内容	投标文件内容齐全、无遗漏。
3	采购文件的响应程度审查	投标文件内容 投标有效期	满足采购文件规定。
4	实质性条款审查	实质性条款是否负偏离	符合采购文件要求的，与采购文件中标注“*”的条款发生实质性无负偏离的情形。

3.澄清问题

由评标委员会对投标文件审查中发现的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，以及评标委员会认为需要进一步确认的其他内容，评标委员会将以书面形式并通过询标的方式要求供应商到场作出必要澄清、说明或者补正。供应商必须按照评标委员会委托采购代理机构通知的时间、地点安排技术或商务人员进行答疑和澄清，未响应澄清安排的通知到场进行答疑和澄清，将被视作自动放弃并承担后果。

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。书面澄清将作为投标内容的一部分。

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。

询标的次序和时间是根据评委对投标文件审查的具体情况安排的，如果评委认为已经理解或不需要澄清的投标文件，将可能不再安排投标人进行询标。

4.详细评审

评标委员会对通过符合性审查的投标文件，依照本办法对技术、商务内容作进一步评审、比较。评标委员会成员经过阅标、审标和询标，对各投标人进行综合打分。

评委打分参照本部分附表：评分标准表。技术商务得分由各评标委员会成员打分，根据投标人的投标文件及相关澄清文件，进行独立打分。价格分由评标委员会统一核算。评委打分采用记名方式，取所有评委汇总得分的算术平均分（小数点后保留二位小数）。

注：评标委员会认为投标文件无效的，应组织相关投标人代表进行陈述、澄清或申辩。

评标委员会认为投标人报价明显低于其它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，必要时提供相关证明材料；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标处理。

采购代理机构可协助评标委员会组长评委对打分结果进行校对、核对并汇总统计；对明显畸高、畸低的评分（其总评分偏离平均分 30%以上的），评标委员会组长评委应提醒相关评标委员会成员进行复核或书面说明理由，评标委员会成员拒绝说明的，由现场监督员据实记录；评标委员会成员的评审、修改记录应保留原件，随项目其他资料一并存档。

5.确定中标候选人名单

本项目由评标委员会推荐 2 名中标候选人。

评标委员会根据投标人的综合得分高低排定顺序，推荐综合得分排名第一的投标人为第一中标候选人，推荐综合得分排名第二的投标人为第二中标候选人。如投标人综合得分相同的则价格低者优先中标；若技术商务得分也相同，则由投标人抽签决定。

采购响应截止时间或评审期间，若出现参与的供应商或者对采购文件作出实质性响应的供应商不足 3 家的情况，该项目招标采购活动终止。

如评标过程中出现本招标文件未尽事宜，则由评标委员会讨论决定。

6.编写评标报告

评标委员会根据全体评标成员签字的原始评标记录和评标结果编写评标报告；评标结束。

四、投标无效的情形

没有响应采购文件实质性要求的投标将被视为无效投标。投标人不得通过修正或撤消不合要求的偏离或保留从而使其投标成为实质上响应的投标。

1.在资格审查时，如发现下列情形之一的，投标文件将被视为无效：

（1）资格证明文件不全的或者不符合采购文件标明的资格要求的；

（2）供应商资格声明函无法定代表人或授权代表签名或盖章；

2.在符合性审查时，如发现下列情形之一的，投标文件将被视为无效：

（1）投标文件未按采购文件要求签署、签章的；

（2）投标有效期不满足采购文件要求的；

（3）明显不符合采购文件要求的，或者与采购文件中标注“*”的条款发生实质性负偏离的；

（4）投标文件中含有采购人不能接受的附加条件的；

（5）委托人未提供法定代表人授权委托书或填写项目不齐全的；

（6）投标文件格式不规范、提供资料不齐全或者内容虚假的；

（7）投标文件的实质性内容未使用中文表述、表述不明确、前后矛盾或者使用计量单位不符合采购文件要求的（经评标委员会认定并允许其当场更正的笔误除外）；

（8）投标文件的关键内容字迹模糊、无法辨认的，或者投标文件中经修正的内容字迹模糊难以辨认或者修改处未按规定签署、盖章的；

（9）法律、法规和采购文件规定的其他无效情形；

3.在技术商务评审时，如发现下列情形之一的，投标文件将被视为无效：

（1）未提供或未如实提供投标服务需求,或者投标文件标明的响应或偏离与事实不符或虚假投标的；

（2）投标技术方案不明确，存在一个或一个以上备选（替代）投标方案的；

4.在报价评审时，如发现下列情形之一的，投标文件将被视为无效：

（1）报价超过采购文件中规定的预算金额或者最高限价的；

（2）未采用招标文件要求的报价形式报价的；

（3）投标报价具有选择性；

（4）评标委员会一致认为报价不合理的（不平衡报价）；

（5）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,有可能影响服务质量或者不能诚信履约的，且不能在评标现场合理时间内提供相关证明材料说明其报价的合理性的；

（6）采购文件规定的其他无效情形；

5.被拒绝的投标文件为无效。

五、评分标准表

评分标准表

序号	评审项目	评分范围	分值
1	整体服务方案	（1）信息资产统计服务方案 评标委员会根据供应商针对招标文件“第二章采购需求”拟定的信息资产统计服务方案，进行综合评议： ①信息资产统计服务方案内容详尽合理预见性强、条理清晰，可行的得 5 分； ②信息资产统计服务方案内容较为详尽合理、条理较清晰，较为可行的得 3 分； ③信息资产统计服务方案内容片面不完整，条理不清晰，表述不够准确到位，存在缺陷的得 1 分； ④未提供的不得分。	5 分
		（2）运维管理建设服务方案 评标委员会根据供应商针对招标文件“第二章采购需求”拟定的运维管理建设服务方案，进行综合评议： ①运维管理建设服务方案内容详尽合理预见性强、条理清晰，可行的得 5 分； ②运维管理建设服务方案内容较为详尽合理、条理较清晰，较为可行的得 3 分； ③运维管理建设服务方案内容片面不完整，条理不清晰，表述不够准确到位，存在缺陷的得 1 分； ④未提供的不得分。	5 分
		（3）服务器运维服务方案 评标委员会根据供应商针对招标文件“第二章采购需求”拟定的服务器运维服务方案，进行综合评议： ①服务器运维服务方案内容详尽合理预见性强、条理清晰，可行的得 5 分； ②服务器运维服务方案内容较为详尽合理、条理较清晰，较为可行的得 3 分； ③服务器运维服务方案内容片面不完整，条理不清晰，表述不够准确到位，存在缺陷的得 1 分； ④未提供的不得分。	5 分

		（4）存储设备运维服务方案 评标委员会根据供应商针对招标文件“第二章采购需求”拟定的存储设备运维服务方案，进行综合评议： ①存储设备运维服务方案内容详尽合理预见性强、条理清晰，可行的得 5 分； ②存储设备运维服务方案内容较为详尽合理、条理较清晰，较为可行的得 3 分； ③存储设备运维服务方案内容片面不完整，条理不清晰，表述不够准确到位，存在缺陷的得 1 分； ④未提供的不得分。	5 分
		（5）网络设备运维服务方案 评标委员会根据供应商针对招标文件“第二章采购需求”拟定的网络设备运维服务方案，进行综合评议： ①网络设备运维服务方案内容详尽合理预见性强、条理清晰，可行的得 5 分； ②网络设备运维服务方案内容较为详尽合理、条理较清晰，较为可行的得 3 分； ③网络设备运维服务方案内容片面不完整，条理不清晰，表述不够准确到位，存在缺陷的得 1 分； ④未提供的不得分。	5 分
		（6）安全设备运维服务方案 评标委员会根据供应商针对招标文件“第二章采购需求”拟定的安全设备运维服务方案，进行综合评议： ①安全设备运维服务方案内容详尽合理预见性强、条理清晰，可行的得 5 分； ②安全设备运维服务方案内容较为详尽合理、条理较清晰，较为可行的得 3 分； ③安全设备运维服务方案内容片面不完整，条理不清晰，表述不够准确到位，存在缺陷的得 1 分； ④未提供的不得分。	5 分

		（7）机房设备运维服务方案 评标委员会根据供应商针对招标文件“第二章采购需求”拟定的机房设备运维服务方案，进行综合评议： ①机房设备运维服务方案内容详尽合理预见性强、条理清晰，可行的得 5 分； ②机房设备运维服务方案内容较为详尽合理、条理较清晰，较为可行的得 3 分； ③机房设备运维服务方案内容片面不完整，条理不清晰，表述不够准确到位，存在缺陷的得 1 分； ④未提供的不得分。	5 分
		（8）桌面终端运维服务方案 评标委员会根据供应商针对招标文件“第二章采购需求”拟定的桌面终端运维服务方案，进行综合评议： ①桌面终端运维服务方案内容详尽合理预见性强、条理清晰，可行的得 5 分； ②桌面终端运维服务方案内容较为详尽合理、条理较清晰，较为可行的得 3 分； ③桌面终端运维服务方案内容片面不完整，条理不清晰，表述不够准确到位，存在缺陷的得 1 分； ④未提供的不得分。	5 分
		（9）高速公路视频资源整合平台维护服务方案 评标委员会根据供应商针对招标文件“第二章采购需求”拟定的高速公路视频资源整合平台维护服务方案，进行综合评议： ①高速公路视频资源整合平台维护服务方案内容详尽合理预见性强、条理清晰，可行的得 5 分； ②高速公路视频资源整合平台维护服务方案内容较为详尽合理、条理较清晰，较为可行的得 3 分； ③高速公路视频资源整合平台维护服务方案内容片面不完整，条理不清晰，表述不够准确到位，存在缺陷的得 1 分； ④未提供的不得分。	5 分

		（10）需充放电设备维护服务方案 评标委员会根据供应商针对招标文件“第二章采购需求”拟定的需充放电设备维护服务方案，进行综合评议： ①需充放电设备维护服务方案内容详尽合理预见性强、条理清晰，可行的得 5 分； ②需充放电设备维护服务方案内容较为详尽合理、条理较清晰，较为可行的得 3 分； ③需充放电设备维护服务方案内容片面不完整，条理不清晰，表述不够准确到位，存在缺陷的得 1 分； ④未提供的不得分。	5 分
		（11）路网中心 GQY 大屏延保服务方案 评标委员会根据供应商针对招标文件“第二章采购需求”拟定的路网中心 GQY 大屏延保服务方案，进行综合评议： ①路网中心 GQY 大屏延保服务方案内容详尽合理预见性强、条理清晰，可行的得 5 分； ②路网中心 GQY 大屏延保服务方案内容较为详尽合理、条理较清晰，较为可行的得 3 分； ③路网中心GQY大屏延保服务方案内容片面不完整，条理不清晰，表述不够准确到位，存在缺陷的得 1 分； ④未提供的不得分。	5 分
2	项目重难点分析及相应的解决方案	评标委员会根据供应商针对招标文件“第二章采购需求”拟定的项目重点、难点分析及解决方案，进行综合评议： （1）对本项目各部分工作内容涉及的关键点、重难点分析全面、透彻，详细描述了解决项目重点难点的具体措施和方法；解决措施详细、切实可行，能够有效解决问题的得 6 分； （2）对本项目各部分工作内容涉及的关键点、重难点分析基本准确，基本覆盖了解决项目重点难点的主要方面，但存在一些遗漏；解决措施具有一定针对性、可行性，并能够达到预期效果的得 4 分； （3）对本项目各部分工作内容涉及的关键点、重难点分析不到位，方案描述较为简略，缺乏具体细节和实施步骤；解决措施粗糙、缺乏针对性或不足以解决问题的得 2 分； 未提供不得分。	6 分
3	内部管理制度	评标委员会根据供应商针对招标文件“第二章采购需求”拟定的内部管理制度，包括但不限于：定期巡检制度和设备运行情况报	6 分

		告制度，日常养护、维修、检测情况报告制度，服务档案和解决方案资料库制度等，进行综合评议： （1）内部管理制度内容全面，各个内容针对性强，各项制度完全能够落实到位的得 6 分； （2）内部管理制度内容较为全面，各个内容针对性较强，各项制度基本能够落实到位的得 4 分； （3）内部管理制度内容不够全面，各个内容针对性较弱，各项制度落实较难的得 2 分； （4）未提供的不得分。	
4	突发风险应急处理预案	评标委员会根据供应商针对招标文件“第二章采购需求”拟定的突发风险应急处理预案，包括但不限于：制定的应急预案是否全面、应急措施是否具体、应急人员的职责是否清晰、临时投入可投入的资源是否充足等，进行综合评议： （1）突发风险应急处理预案全面详实，有针对性分析，应急措施足够具体，应急人员的职责非常清晰，临时投入可投入的资源非常充足的得 6 分； （2）突发风险应急处理预案较为详实，有一定分析，应急措施较为具体，应急人员的职责较为清晰，临时投入可投入的资源较充足的得 4 分； （3）突发风险应急处理预案不够详实，分析混乱，应急措施不够具体，应急人员的职责模糊不清，临时投入可投入的资源比较匮乏的得 2 分； （4）未提供的不得分。	6 分
5	人员配备	（1）供应商拟派的项目负责人具有注册信息安全专业人员证书的得 1 分，具有 5 年以上信息化领域从业经历的得 1 分，10 年及以上信息化领域从业经历的得 2 分；满分 3 分。 （2）供应商拟派的项目技术负责人同时具有注册信息安全专业人员证书及工信部网络工程师证书的得 2 分，具有 5 年以上信息化领域从业经历的得 1 分；满分 3 分。 **注：提供人员证书、加盖投标人公章的从业经验证明和开标前近 3 个月社保证明材料并加盖供应商公章。**	6 分
6	备品备件库	供应商具有备品备件库且能满足招标文件“第二章 采购需求”《备品备件清单》的得 5 分，备品备件不全的每缺少一项扣 1 分，扣完为止。	5 分
7	企业实力	（1）信息技术服务管理体系认证证书；	3 分

		（2）信息安全管理体系认证证书； （3）质量管理体系认证证书； 供应商具有上述证书的每项得 1 分，满分 3 分。（提供证书复印件加盖单位公章）	
8	类似项目经验	2022 年 1 月 1 日（以合同签订日期为准）-至今，供应商承担过信息化运维类合同业绩的每个得 0.5 分，满分 1 分。 注：需提供同复印件加盖单位公章，未提供不得分。	1 分
9	价格分	满足招标文件要求且参与评审价格最低为评标基准价，其价格分为满分。 其他供应商的价格分按照下列公式计算： 参与评审价格=通过报价评审且有效的投标价格 价格分=（评标基准价/参与评审的价格）×12 投标报价得分以四舍五入保留小数点后二位。	12 分
合计			100 分

评委签字：

日期：　　年　　月　　日

第五章　合同主要条款

信息化设备及安全服务外包项目承包合同

甲方（发包人）：宁波市公路与运输管理中心（以下简称甲方）

乙方（承包人）：_____（以下简称乙方）

根据信息化设备及安全服务外包项目（项目编号：_____）公开招标结果，确定由乙方中标。按照《中华人民共和国民法典》的有关规定，在自愿、平等、公平、诚信的基础上，经双方协商一致，签订本合同。

一、项目概况

（一）IT 维护技术服务项目内容：

信息资产统计服务、运维管理建设服务、服务器运维服务、存储设备运维服务、网络设备运维服务、安全设备运维服务、机房设备运维服务、桌面终端运维服务等内容。

（二）服务地点及范围

1、路网大楼

序号	设备名称	数量
1	桌面设备，办公电脑，及打印机等桌面周边设备	约 40 台
2	核心机房 IT 设备包含服务器，存储，网络设备等	总数约 170 台
3	UPS 系统（需提供配件包含电池组更换服务）	3 套（路网中心机房 2 套，3 楼指挥中心 1 套）
4	精密空调（每年提供两次精密空调外机清洗服务，及空调过滤网更换服务。）	4 台
5	机房基础设备,包含消防系统，机房内部安防系统，环境动力监控系统，机房照明系统，路网中心综合布线系统。	1 套
6	针对公路运输中心一批需充放电的设备进行定期充放电维护，（需提供锂电池的更换服务）	239 台
7	对路网中心视频会议终端设备进行运维，包括专业巡检、系统调优、数据维护、重大事件现场支持。对会场话筒、大屏、音响、大屏系统、线缆等辅助设备进行日常运维，对损坏的设备进行维修更换。涉及路网中心视频会议设备日常运维、设备运维等。无偿提供具有原厂或与原厂同等级的技术支持。	1 套

2、中心大楼

序号	设备名称	数量
1	桌面设备，办公电脑，及打印机等桌面周边设备	约 130 台
2	机房 IT 设备主要有网络设备等	总数约 10 台

3	UPS 系统	1 套
4	精密空调	2 台
5	机房基础设备,包含消防系统，机房照明系统，综合布线系统。	1 套

3、路政大楼

序号	设备名称	数量
1	桌面设备，办公电脑，及打印机等桌面周边设备	约 150 台
2	机房 IT 设备主要有网络设备等	总数约 10 台
3	UPS 系统	1 套
4	精密空调	1 台
5	机房基础设备,包含消防系统，机房照明系统，综合布线系统。	1 套

4、高速公路视频资料整合平台（10 个下属单位）

序号	设备名称	数量
1	海康威视 DVR 等视频周边设备	约 20 台

5、路网中心 GQY 大屏延保服务

序号	设备名称	数量
1	72 英寸 DLP 大屏	32 块
2	大屏控制管理软件	1 套
3	高分应用平台（含多媒体接入、交通综合管理可视化信息）	1 套

6、信息安全运维外包服务

序号	服务内容	数量
1	宁波市公路与运输管理中心信息安全运维服务	1 项

注：以上运维中涉及的产品均需提供配件更换服务，配件更换费用由乙方承担，甲方无需再支付费用。

二、运维方式及人员要求

1、针对中心大楼、路政大楼、路网大楼的数据中心机房及桌面端维护，供应商需分别各驻场 1 名外包服务工程师。1 名机动工程师，负责 10 个高速公路业主公司及中心关联企业内中心所属信息化设备的运维服务。

2、针对信息安全运维服务供应商需指定驻场 1 名具有中国信息安全测评中心认证的注册信息安全管理人员证书及工信部网络工程师证书的安全运维工程师。

3、为确保调度大屏的正常运行，针对路网中心 GQY 大屏延保服务供应商应提供 1 名技术工程师实现 24 小时应急响应服务。

4、项目团队须配备一名项目负责人总体负责本项目的管理和协调，项目负责人须有 3 年以上信息化领域从业经历，常驻宁波。项目负责人应覆盖硬件设备运维管理的相关技术领域，包括服务器、存储、网络和安全设备、数据库等。

5、项目团队须制定一名项目技术负责人，项目技术负责人应覆盖硬件设备运维管理的相关技术领域，包括服务器、存储、网络和安全设备、数据库等。

6、项目团队须指定一名项目投诉处理人（非项目协调人），以完成本项目的质量监控，提供联系电话。针对项目投诉必须在 24 小时内给出书面答复。

7、对于中标单位派驻的驻场服务人员及机动人员，如不满足用户的人员要求，用户有

权要求更换人员，直到符合用户需求为止。原则上已符合用户要求的的派遣人员，中标单位不得随意更换，如确因故调换已有运维人员，中标单位须在实施调换前 15 个工作日书面通知用户，在征得用户同意的情况下方可进行调整，调换后的运维人员技术水平不得降低。

三、具体运维服务要求

（一）信息资产统计服务

1、维保服务内容：

通过 IT 运维系统建立完善的设备档案(包含在运维数据库中），为以后的配置的变更管理和其他 IT 维护服务的顺利进行打下良好的基础。IT 运维系统资产管理应包括：

标记设备：计算机及外设设备、网络设备、安全设备服务器及存储等 IT 系统设备进行统一的资产登记，并建立唯一标号；

建立设备配置文档：网络设备、安全设备服务器及存储的配置信息进行记录和分析，建立硬件设备配置档案；

网络地址管理列表：IP 地址、子网地址、VLAN 进行统一的规划和分配，并建立管理文档。

（二）运维管理建设服务

为规范化宁波市公路与运输管理中心信息系统的运维和管理工作，协助用户建立整体性运维体系，规范运维流程管理、运维资料管理、运维事件管理、系统监控管理等过程。本项目要求供应商在服务期限内提供 IT 运维一体机服务，其技术参数要求如下：

指标项	指标要求
一、总体架构	
系统架构	采用 B/S 架构，支持中文管理界面。
部署方式	支持集中式和分布式部署方式，实现跨机房的数据中心运维监控。
	监控对象采用无代理方式部署，支持 SNMP、SSH、JMX 等采集模式，采集过程要求不影响监控对象的性能。
	可以作为数据中心服务平台单独使用，也可以作为运维云的线下服务终端使用。
权限	按不同用户角色，分配监控对象和视图查看权限，实现用户角色和监控对象、视图的查看权限关联
二、功能	
数据库监控	支持 Oracle、SQL Server、MySQL、DB2 等数据库。
	支持数据库运行健康状态监控，包括： 可用性监控：监听、实例、表空间的可用性； 错误监控：数据库运行过程中的错误数量； 性能监控：数据块逻辑读指标直观反映数据库性能； 变化监控：对象（表、索引、视图等）、权限（用户、表）、空间（对象、表空间、归档）的变化量； 可靠性监控：备份及容灾系统的运行状态。
	支持 SQL 执行生命周期完整监控，包括：登录、解析、执行、提交。 通过 SQL 执行次数、SQL 执行时间，主观展示 SQL 执行性能瓶颈。

	支持数据库关联资源监控，包括： 数据库资源监控：processes、session、DB files、jobs。 三大资源锁监控：Mutex、 Latch、 Lock。 主机资源监控，包括：CPU、内存、存储、网络。
数据库巡检	支持 2 个对象的业务系统、数据库类型、实例名、操作系统、IP 地址、巡检完成时间等信息进行全面巡检 支持巡检对象的异常信息数量统计，运维人员可及时掌控各系统数据库的健康状况整合资深数据库专家的多年运维经验，形成专家智能系统，根据数据库的健康状态，给出专业的分析，对数据库可能存在的故障和问题进行快速定位，对每个异常指标提供专业解读和排错建议 1.支持一键操作实现全面巡检 2.全面巡检的报告内容至少包括：数据库可用性、空间管理、安全性、可靠性、性能、错误、主机资源、数据库资源、数据库软件、数据库参数、系统参数等信息 3.支持在线和以 PDF 文档导出两种方式查看巡检报告
数据中心监控	支持 WebLogic、Tomcat 等主流业务中间件监控。采用 JMX 直接监控 Java 应用程序服务器的功能，无需第三方模块或集成层。使用高效的 Java 网关监视 Tomcat 等应用服务器，包括：JVM 可用内存、JVM 最大内存、JVM 总的内存、线程等。
	支持 Linux、Windows、AIX、HP-UX、Solaris 等操作系统监控。监控操作系统的运行状态，包括：主机状态、CPU 利用率、内存利用率、磁盘 I/O 读写速率、磁盘 I/O 读写速率，网络 I/O 等。
	支持 VMware 虚拟机状态监控，包括：VMware 物理主机硬件状态、虚拟机在线状态、CPU 利用率、内存大小及利用率、磁盘空间大小及利用率等。
	支持 IBM、HP、DELL、联想、曙光、浪潮等主流物理服务器监控，包括对服务器的硬件状态进行自动告警，包括：CPU、硬盘、电源、风扇、RAID 卡等。
	支持 EMC、NetApp、IBM、华为等主流存储设备监控，包括：存储系统的磁盘、存储控制器、电源、风扇等运行状态。
	支持华为、H3C、思科、锐捷等主流网络设备监控，包括监控网络设备的在线状态。对网络线路运行状态监控，包括线路连通性、线路响应时间、线路流量、线路带宽利用率、线路错包率、线路丢包率等信息。对网络设备接口状态进行监管，包括接口状态、接口流量性能等信息。
触发模式	支持人工阀值模式，可自由设置告警触发阀值库。 支持智能诊断模式，采用大数据技术和机器学习技术，智能识别异常，并发送警告。
监控视图	预先封装不同监控对象的大屏展示模版，包括：中间件、数据库、操作系统、虚拟机、物理服务器等。实现常见运维故障（80%以上）及隐患能从大屏中直观展示及告警。 支持按照业务角度进行关联视图定制。 支持按照资源种类进行分类和关联视图定制。 支持机柜图、系统拓扑图、网络拓扑图等视图定制。 其中数据库监控模版，要求实现： 1.一张大屏可以直观显示监控对象的健康指数，并根据阀值自动告警。 2.从流程及时间模型的角度联动展示各项指标，清晰定位问题环节。
运维云服务	提供和运维一体机配套的线上运维云服务，实现告警订阅、告警推送、工单流转、数据库专家在线服务等功能
	运维云服务采用多租户方式交付，不同租户之间安全隔离。 运维一体机采用加密通道方式和运维云单向连接。

	可定义告警推送和服务人员接收的对应关系，包括：告警站点、告警级别、通知方式等。
	按运维对象的重要性和故障级别，可定义不同的告警通知级别。 告警通知方式支持：邮件、微信、APP。 支持告警通知升级机制。
	提供待处理告警列表，服务人员快速查阅需要处理但还未处理的告警。 采用大数据结构的集中管理模式，支持告警日志的高效查询、分析。 告警日志保存时间要求至少 13 个月以上。
	提供新建工单、工单流转、工单升级、工单统计报表等功能。 与告警订阅和服务授权紧耦合。 针对“待处理告警”，支持一键发起服务工单。
	提供数据库巡检和 AWR 报告解读工具，支持离线上传采集包和 AWR 原生报告，自动生成巡检报告和 AWR 解读报告。
	可单独订购远程数据库专家服务。 通过把数据库告警同步推送给线上数据库专家，并上传诊断资料包，数据库专家结合告警内容和诊断资料包进行分析，给出解决方案和交付服务。
三、产品规格与授权	
产品形态	软硬件一体机方式
硬件指标	1U 机架式 内存≥8G 存储空间≥500G 至少提供 4 个网口
授权数量	支持 8 个数据库实例，100 个监控节点

（三）服务器运维

1、维保服务内容

本次维保包括现有清单所列服务器以及服务期内新增服务器的硬件维保服务，维保期间的故障部件更换费用由投标单位承担。

（1）日常维护

包含设备的检测、维护、维修、搬迁，以及操作系统安装、设备软硬件的配置调整、设备固件版本升级等。所需备品和耗材由中标方免费提供，提供人员驻点服务。

必须提供巡检项目记录表。巡检结束后由技术人员和招标单位指定人员签字，当场提交巡检记录表。

2、服务响应及服务人员

要求提供 7×24 小时服务，电话响应在 15 分钟以内，电话支持无法解决问题的情况下 1 小时内到达现场。确定为硬件故障需要更换的，在备件到位后 12 小时内解决故障问题。维护完成后当场提交服务报告，由服务人员和甲方指定人员签字确认。故障件更换需提交部件设备更换单，并载明原部件型号及序列号、更换部件型号及序列号等内容。

乙方需提供指定服务人员的资质、多种联系方式，未经甲方同意乙方不得随意调整指定服务人员。

（四）存储

1、维保服务内容

本次维保包括现有清单所列存储设备以及服务期内新增存储设备的软硬件维保服务以及定期巡检服务。

（1）主动运维服务

为减少存储故障对业务工作的影响，需要乙方提供主动运维服务，在甲方未发现故障的情况下能提前或主动发现存储存在的问题。

（2）软硬件日常维护

包含设备的检测、维护、维修、搬迁、以及存储空间的调整分配、数据迁移、数据备份、设备固件版本升级及其他软硬件配置等。

更换备件部件费用由投标单位承担，所供备件需为原厂，不得提供假货，水货，返修货等不良备件。

对设备进行日常维护时，乙方应遵循甲方的时间安排。日常维护工作结束后需马上提交问题原因及解决报告。

（3）定期巡检服务

巡检服务必须在现场进行，标书中必须提供巡检项目记录表。巡检结束后当场提交巡检记录表，由巡检人员和招标单位指定人员签字。

2、服务响应及服务人员

要求提供 7×24 小时服务，电话响应在 15 分钟以内，电话支持无法解决问题的情况下 1 小时内到达现场。维护完成后当场提交服务报告，由服务人员和甲方指定人员签字确认。对已发现存在故障需要更换的部件，一般情况应在备件部件到位后 12 小时内完成，当场提交部件设备更换单，并载明原部件型号及序列号、更换部件型号及序列号等内容。

（五）网络设备

1、维保服务内容

包含设备的检测、维护、维修、搬迁，硬件产品固件升级、软件产品版本升级、特征库升级，以及安全策略调整、系统优化、软硬件配置调整等。

更换备件部件费用由投标单位承担，所供备件需为原厂，不得提供假货，水货，返修货等不良备件。

对设备进行日常维护时，乙方应遵循甲方的时间安排。日常维护工作结束后需马上提交问题原因及解决报告。

2、服务响应及服务人员

要求提供 7×24 小时服务，电话响应在 15 分钟以内，电话支持无法解决问题的情况下 1 小时内到达现场。维护完成后当场提交服务报告，由服务人员和甲方指定人员签字确认。对已发现存在故障需要更换的部件，一般情况应在备件部件到位后 12 小时内完成，当场提交部件设备更换单，并载明原部件型号及序列号、更换部件型号及序列号等内容，由服务人

员和甲方指定人员签字确认。

若故障影响重要业务运行且无法在 12 小时内修复的，中标方需在 12 小时内提供应急的备机备件保证业务正常运作。

日常维护必须指定至少 1 名或以上固定技术人员，技术人员需具备工信部网络工程师证书，固定人员在服务期间不得随意更换，如若更换需具备同等资格证书及技术水平，并取得招标单位同意。

（六）安全运维服务要求

1、信息系统安全服务对象

服务对象是宁波市公路与运输管理中心网络安全运维服务，主要包括交通专网、政务外网和市政务云相关信息系统，应对主要信息系统进行定期安全巡检和维护，及时处理系统安全隐患。

2、驻场服务人员要求：

（1）本次安全服务需一位驻场人员，负责信息系统安全运维。要求具有中国信息安全测评中心认证的注册信息安全专业人员工程师证书及工信部网络工程师证书

工作模式：软件辅助与人工巡查相结合；

运维报告：每周提供信息安全运维周报，每月综合性的月报，半年报和全年信息安全运维总结报告等。

3、服务目标及内容综述

（1）服务目标：保证公路运输中心信息系统整体安全稳定运行及满足公安部信息安全等级保护 2 级要求和政府信息系统安全检查要求。

（2）提供对机房和设备运行状况检查，处理各类网络病毒或木马事件；

（3）建立宁波市公路运输中心系统物理设备（包括网络设备、安全设备、服务器设备、终端、存储备份设备、软件安装媒介）档案；

（4）提供宁波市公路运输中心信息系统的安全状况监测、漏洞扫描、安全加固等信息安全运维服务，按要求进行病毒查杀和日志检查，安全审计和日志分析、病毒日志分析、病毒和漏洞公告，确保网络的安全平稳运行；

（5）针对漏洞扫描中出现的安全隐患、对中心现有网络环境的安全风险进行综合分析评估，并制定对应措施和应急方案；配合宁波市公路运输中心进行等保测评工作。

（6）负责制定宁波市公路运输中心业务网应急响应预案，并在应急事件发生时按照预案进行事件处理，保护关键业务免受重大故障或灾难的影响；

（7）为宁波市公路运输中心软硬件平台建设提供安全咨询及服务；

（8）提供宁波市公路运输中心安全方面的不同层次的知识培训，增强信息安全意识。

（9）提供 7*24 小时网站安全服务，保障网站业务的连续性，对出现问题及时解决。

4、服务方式与内容：

（1）日常设备安全监控运维服务

网络设备安全维护：网络设备的日常安全监控，监控重要运行信息，网络链路的连通状态，发现问题及时向公路运输中心安全管理人汇报并协助处理各类网络设备故障和骨干网络链路故障。定期对网络设备监控记录和日志进行分析，发现系统存在的故障隐患和安全隐患，并提出解决建议。

安全设备维护：检测安全设备工作状态和工作性能，及时升级系统软件，并记录备案，及时处理各类安全设备故障。实时监控各项数据和敏感信息，及时发现问题和安全隐患，并做出相应处理，保障网络通讯安全。对安全设备的参数和配置进行动态的管理，维护配置文档和管理文档，并定期备案。

服务器设备安全维护：监控服务器系统运行情况，查看重要系统参数，并做好记录；维护系统注册表，检查操作系统补丁状况，协助安装操作系统补丁，处理各类操作系统使用问题，监控记录和系统相关日志进行分析，及时发现安全漏洞和安全隐患，及时处理各类服务器软硬件故障。动态管理服务器配置文档，并及时更新发生变化的配置项。定期对服务器维护数据进行统计、分析，并提供设备配置、升级建议。

安全评估及新系统上线评估：服务方需参照 GB/T 20984-2007《信息安全技术 信息安全风险评估规范》国家标准，每年进行一次安全风险评估，通过资产评估、脆弱性评估和威胁评估对现有信息系统和网络可能存在的安全风险进行综合分析评估，并提供相应的风险处置建议；同时，要求服务方对宁波市公路运输中心新上线系统提供评估，保证新系统安全，要求输出评估报告。

基线维护及安全加固：服务方需分析客户信息系统的安全需求，结合本行业等级保护基本要求，建立信息系统安全基线，并在服务期内提供维护管理；同时根据安全基线要求提出详细的安全加固建议，制定严谨的加固实施方案，详细记录判断依据、实施步骤、测试与回退方案等内容，确保加固过程安全、有效，且风险可控。

（2）系统安全巡检

主机漏洞扫描：每季度一次对服务器进行漏洞扫描，掌握服务器的安全状况，要求服务方提供主机漏洞扫描报告。

设备健康巡检：每季度一次对设备进行健康检查，对设备进行配置备份，当发现异常情况时，及时进行跟踪处理。

日志安全审计：每季度一次对设备的防护日志进行审计分析，发现系统威胁来源及威胁类型，及时调整安全防护策略以达到安全防护的目的。

（3）应急响应和应急保障

响应支持级别：服务方针对网络和信息系统突发的重大故障和安全事件提供 7*24 小时的服务，30 分钟赶到现场进行故障排查定位，全力恢复网络和系统正常工作，同时查明故障或入侵来源、时间，并提供应急处置报告。

预案维护：根据宁波市公路运输中心提供的信息系统实际情况，结合当前网络环境及政策法规要求，适时修订应急预案。

应急演练：每年一次协助宁波市公路运输中心对信息系统进行相关的应急模拟演练，并对演练中发现的问题进行总结，演练结束后根据发现的问题进行预案的改进。

（4）不定期安全服务

安全咨询服务：为宁波市公路运输中心网络软硬件平台建设提供信息系统相关安全咨询服务。

系统集成咨询服务：为宁波市公路运输中心评估现有及将来的信息化要求，提出切合实际应用的规划书，并为宁波市公路运输中心的信息化信息安全建设提供建议。可应客户要求，对于新上线的系统，进行信息安全测试，并形成报告书。

安全通告服务：总结最新的安全漏洞信息、黑客攻击方法、流行病毒信息、补丁信息、安全发展动态、浙江省内重大安全事件、安全法律法规等安全资讯，以邮件的方式发送给用户，帮助用户集中了解最新的安全动态。根据事件原因及攻击方法，对网站调整提出专业意见。

（5）专项安全检查

每半年一次协助宁波市公路运输中心对区县公路系统进行检查，协助制订检查方案，安排技术人员到场进行检查支持。检查完成后形成综合分析报告，并针对检查中发现的风险提供整改建议方案以及协助完成整改工作。

每半年一次对宁波市公路运输中心区县公路可互联网访问的信息系统进行应用安全检测，服务方需提供检测分析报告，并协助各单位进行漏洞修复、验证。

在每轮检查完成后，服务方需为宁波市公路运输中心提供检查总结培训，培训内容包含但不限于信息安全意识、信息安全技术、国际和国家层面安全态势等。

（6）统一威胁探针

类别	参数	功能及技术描述
威胁检测	流量采集	支持导入 HTTPS 证书，对流量进行解密和还原。
		支持常见应用的识别不低于 3000 种
		支持流量白名单，过滤掉不关注资产流量，白名单类型应包括 IP、端口、邮箱、域名。
	入侵检测	应覆盖多种攻击特征，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测，攻击特征库数量至少为 8000 种以上。
	扫描检测	支持自定义 TCP/UDP 端口扫描检测模型，结合模型对流量进行检测和告警。
		支持自定义 TCP 端口扫描检测模型，支持配置参数包括检测阈值、检测周期、复位时间，提供默认配置。检测产生的告警信息至少包括扫描类型和扫描事件名称。
		支持自定义 UDP 端口扫描检测模型，支持配置参数包括检测阈值、检测周期、复位时间，提供默认配置。检测产生的告警信息至少包括扫描类型和扫描事件名称。

		内置 WEB 应用机器学习检测模型，支持对 sqli，xss，exec，phprce，ptravel 和 jeli 攻击类型进行分类检测和告警，告警信息至少包括机器学习告警类型和威胁事件名称。
	WEB 应用检测	WEB 类告警详情中包含请求和响应信息，在请求和响应信息中能标记规则匹配中的字段信息，便于运维人员快速进行确认攻击事件。
		支持 WEB 类的攻击结果进行判定
	恶意文件检测	内置恶意文件检测引擎，支持对可执行文件、文档、压缩包和网页脚本进行恶意代码检测和告警，告警信息中至少包含恶意文件类型、恶意文件家族信息和恶意文件变种信息。
	威胁情报检测	支持与威胁情报联动，可进行实时流量匹配检测和告警，支持对恶意 IP、恶意域名、恶意 URL 和恶意文件进行检测。
	WEBshell 检测	内置基于统计学特征和操作码序列训练的检测模型，支持对 asp、jsp、php 文件类型进行检测和告警 内置基于 webshell 通信特点以及流量特征构建决策模型，支持对 asp 文件、php 文件、jsp 文件和图片马进行检测和告警 告警信息至少包括机器学习告警类型和威胁事件名称
	异常行为检测	支持自定义 TCP/UDP 行为检测模型，通过自定义内部资产对流量中的异常行为（包括内部向外部发起、内部对内部发起）进行检测和告警，告警信息包含检测类型和威胁事件名称。
		支持自定义 TCP 行为模型，配置参数至少包括检测阈值、检测周期、复位时间、IP 对象。
		支持自定义 UDP 行为模型，配置参数至少包括检测阈值、检测周期、复位时间、IP 对象。
威胁展示		支持展示威胁告警信息，展示的告警分类包括入侵检测告警、WEB 应用告警、恶意文件告警、威胁情报告警。
	入侵检测告警	入侵检测告警字段至少包括：告警时间、攻击 IP、攻击端口、受害 IP、受害端口、告警类型、事件名称、威胁等级、详情。
	WEB 应用告警	WEB 应用告警字段至少包括：告警时间、攻击 IP、攻击端口、受害 IP、受害端口、告警类型、事件名称、URI、威胁等级、详情。
	恶意文件告警	恶意文件告警字段至少包括：告警时间、攻击 IP、攻击端口、受害 IP、受害端口、传输协议、应用层协议、文件类型、文件名、文件 md5、详情。
	威胁情报告警	威胁情报告警字段至少包括：告警时间、攻击 IP、攻击端口、受害 IP、受害端口、告警类型、事件名称、命中的威胁情报、详情。
回溯分析		应具备元数据提取、存储和检索的能力。
		支持元数据存储和展示，元数据类型至少包括 TCP&UDP 日志、HTTP 日志、EMAIL 日志、FTP 日志、DNS 日志、ICMP 日志、文件还原日志。
响应		支持对入侵检测告警、WEB 应用告警、威胁情报告警和恶意文件告警中的攻击 IP 和受害 IP 发送阻断报文，进行旁路阻断。
		支持自定义一键封堵，配置策略包括 IP 类型（配置选项包括源 ip/源端口/目的 ip/ 目的端口）、域名类型、生效时间和失效时间。

		支持与大数据平台联动：提供 API 接口，由大数据平台通过接口下发一键封堵断策略，探针执行封堵动作并将封堵日志信息发送给大数据平台。
取证（流量存储）		支持对采集的全部流量进行存储、检索和下载，检索条件包括源 IP、目的 IP、源端口、目的端口、起止时间。
		支持自定义规则抓取和留存可疑原始流量，自定义规则支持对原始流量的 payload 进行匹配。自定义规则内容至少包括：源 IP/源端口、目的 IP/目的端口、匹配类型（二进制、字符串、正则表达式）、匹配特征、会话数量、过期时间。
资产识别		支持从流量中识别资产信息和展示，识别的信息至少包括资产 IP、资产 MAC、服务端口号、服务协议、设备类型、地理位置、操作系统、资产状态、资产描述、资产关联账号。
系统管理	备份	支持配置策略的备份，备份数据至少包括全部配置、引擎参数、接口参数和白名单。
		支持备份策略恢复，恢复的类型包括全部配置、引擎参数配置，接口参数配置和白名单配置。
	二次开发	具备二次开发能力，支持第三方通过探针的标准接口进行新的业务开发。
部署能力	部署模式	系统应支持监听（Monitor），能够快速部署在各种网络环境中。
	网络适应能力	系统支持旁路部署，支持 IPv4/IPv6 环境部署。
		系统应支持 VLAN 802.1Q、BGP、MPLS、QinQ、PPPOE 等封装协议，能够适应多种不同的网络环境。

（7）安全威胁监控及响应服务

序号	服务名称	服务数量	说明
1	威胁监控与分析服务	1 年	搭建专业的监控分析平台； 提供 7*24 小时全天候的威胁监控与分析服务；及时对互联网区业务上的威胁事件作出应急响应； 提供专家服务，对热点事件进行预警与防护，对高危访问源进行监控与封杀，对可疑安全事件进行发现与确认。
2	应急响应及技术支持服务	1 年	对突发的安全事件进行响应； 提供应急响应服务，第一事件提供现场应急响应服务和远程技术支持服务； 重保时期，提供现场 7×24 小时的保障服务； 及时提供最新漏洞的检查方式、加固建议等。
3	专业的监控分析平台	1 年	一年租赁费用（整体平台及设备需部署在用户内网）

服务要求

采取人工监控和工具分析相结合的方式对甲方开展 7*24 小时威胁监控与分析工作；监控工程师必须是乙方工程师，需提供社保证明；熟悉甲方现有的网络安全平台，能熟练使用甲方指定的关键网络安全设备，对设备产生的日志告警事件进行分析，并及时作出处置。

服务内容

以甲方现有互联网域的网络安全防护体系为基础，在本地安装部署专业分析工具，搭建专业的监控分析平台，配置合适的威胁监测及分析的模板。

监控分析平台至少包括智能安全运营平台、统一威胁分析系统、漏洞扫描系统等软件、

硬件设备，须实现如下功能：

平台功能	功能要求
智能安全运营平台	平台支持分布式部署，同时支持软件、硬件的形式部署；能够与监控平台中的统一威胁分析、漏洞扫描、代码审计等系统进行联动，对甲方的数据进行采集、分析、处置。 支持多种协议数据的接入，默认内置至少 300 种各厂商设备日志类型的解析规范化规则，支持甲方现有安全设备的数据接入。 支持资产风险识别，能够实现资产的多维度管理，系统至少内置五种视图：资产组视图、业务系统视图、组织结构视图、地理位置视图、行业视图。 支持漏洞监测分析，能够联动漏洞扫描系统，针对操作系统、业务等自动下发漏动扫描任务，对结果进行展示、分析、建议。 支持日志威胁检测分析，内置不少于 200 种内置分析规则并支持规则库的升级，对可疑安全事件能够按业务系统、网站、终端三种视角进行威胁分析以攻击链阶段统计和展示。 支持对流量日志的分析，发现其中的可疑行为，内含不少于 25 种内置可疑行为分析场景，可疑分析场景包括但不限于：风险账号、内部访问异常、数据泄露等，内置场景支持升级；支持流量数据的查询分析能力，提供会话日志和相关协议日志的关联分析。 平台能结合甲方现有的安全设备，进行全面、综合地分析，主动发现网络中可能存在的安全威胁和安全隐患，评估并展示安全治理等；及时对安全威胁事件作出判断、告警、溯源分析，并提供一键封堵、一键解封等功能的自动处置功能。
统一威胁分析系统	以硬件设备形式接入，要求设备性能满足内存>=32G，硬盘>=4T，吞吐量>=9.8G，最大并发 TCP 会话数>=280 万，每秒新增 TCP 会话数>=60000。 系统支持导入 HTTPS 证书，对流量进行解密和还原；能够针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量、TCP/UDP 的异常行为进行检测，攻击特征库数量至少为 8000 种以上，并对威胁异常行为进行回溯取证分析。 系统支持入侵检测、扫描检测、web 应用检测、恶意文件检查、威胁情报检测、webshell 检测、异常行为检测，并对检测结果进行分析，将威胁告警信息进行分类展示。 系统支持资产的识别，识别的信息至少包括括资产 IP、资产 MAC、服务端口号、服务协议、设备类型、地理位置、操作系统、资产状态、资产描述、资产关联账号。 系统支持溯取证分析，能对采集的全部流量进行存储、检索和下载。
漏洞扫描系统	支持资产的识别和分析，能够对资产进行分级分类管理。 支持检测的漏洞数大于 120000 条，兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准；支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息； 支持扫描大数据组件框架的漏洞，需覆盖 Ambari、Cassandra、Elasticsearch、Flume、Hadoop、Hbase、Hdfs、Hive、 Impala、Kafka、Mongodb、Oozie、Redis、Spark、Storm、Yarn、Zookeeper，要求能够扫描大于 200 条相关漏洞； 支持扫描国产操作系统、应用及软件的安全漏洞，如红旗、麒麟、起点操作系统。 支持扫描主流云主机机管理系统的安全漏洞，如：VMWareESX/ESXi、KVM、Xen，要求能够扫描大于 4000 条相关漏洞。 支持专门针对已有攻击利用代码的漏洞检测，检测用户资产是否存在可利用的漏洞。

①提供 7*24 小时威胁监控、分析服务，对专业工具、网络设备 WAF、IPS 等设备的安全

告警进行分析、处置；根据威胁分析结果及时对安全设备策略进行优化，对高危访问源进行监测、封杀；每日提供一份当日监控运维报告（周一至周五，前一天 18:00-当日 9：00；周末全天）。

②针对攻陷类事件进行通告，并对事件的处置情况进行追踪，定期对事件统计分析并反馈事件的处置结果，每周一次。

③提供专家服务，对安全威胁及事故进行调查取证，并提供处置建议。实现热点事件的预警与防护、高危访问源的监测与辅助封杀处置、可疑安全事件的发现与确认。每周至少一次。具体提供的服务内容：

工作内容	工作要求
热点事件的预警与防护	出现热点事件时，及时通过电话、短信、邮件等方式向，将安全事件相关背景信息、漏洞与攻击相关特征及通用处置建议发送给甲方；可在甲方授权下，对安全检测和防护类设备的规则库进行升级并配置安全防护策略。
高危访问源的监测与封杀	利用监控平台及甲方的各类安全设备，及时发现潜在的攻击者，在攻击者找到攻陷方法或路径之前，针对访问源进行拦截。
可疑安全事件的发现与确认	采用互联网边界访问行为检测与流量深度分析相结合的方式，通过系统攻击检测、web 攻击检测、网站安全监测（或通告）和威胁情报等方式，帮助发现并确认可疑的安全事件；快速对可疑事件进行排查和确认，在排查确认后快速向甲方发起安全事件通告，并开始启动应急响应。

（七）机房设备

1、维保服务内容

（1）包扩精密空调、UPS、环境监控、配电等机房设备的检测、维护、维修、清洁、防护、搬迁等。

（2）更换备件部件费用由投标单位承担，所供备件需为原厂，不得提供假货，水货，返修货等不良备件。

（3）每年提供两次精密空调外机清洗服务，及空调过滤网更换服务。

（4）对设备进行日常维护时，乙方应遵循甲方的时间安排。日常维护工作结束后需马上提交问题原因及解决报告。

2、服务响应及服务人员

服务响应为 7×24 小时，电话响应时间 15 分钟，电话支持无法解决问题的情况下现场到达时间为 1 小时，一般故障修复时间为 4 小时，重大故障须与招标单位协商，尽快解决。

（八）桌面设备

1、维保服务内容

（1）包含计算机及打印机等设备的检测、维护、维修、清洁、防护、搬迁等。

（2）对设备进行日常维护时，乙方应遵循甲方的时间安排。日常维护工作结束后需马上提交问题原因及解决报告。

2、服务响应及服务人员

服务响应为 7×24 小时，电话响应时间 15 分钟，电话支持无法解决问题的情况下现场到达时间为 1 小时，一般故障修复时间为 4 小时，重大故障须与招标单位协商，尽快解决。

（九）高速公路视频资源整合平台

1、维保服务内容

（1）包含设备的检测、维护、维修、清洁、防护、搬迁等。

（2）更换备件部件费用由投标单位承担，所供备件需为原厂，不得提供假货，水货，返修货等不良备件。

（3）对设备进行日常维护时，乙方应遵循甲方的时间安排。日常维护工作结束后需马上提交问题原因及解决报告。

（4）维护地点为：宁波市境内高速公路 7 家业务单位 10 个监控中心，具体位置如下：

序号	高速公路业主	监控中心所在地
1	宁波北仑港高速有限公司	甬台温宁波东出口
2	浙江宁波甬台温高速公路有限公司	宁海桑洲（桑洲岭隧道管理所）
3	宁波剡界岭高速公路有限公司	甬金溪口东出口
4	宁波海运明州高速公路有限公司	绕城宁波西出口/甬金宁波西进口
5	宁波市杭州湾大桥发展有限公司	杭州湾大桥庵东出口下去
6	浙江沪杭甬高速公路股份有限公司	杭甬段塘出口
7	宁波交投营运服务有限公司	绕城宁波北出口
8		绕城东东钱湖监控中心(绕城东钱湖出口）
9		象山港大桥咸祥出口
10		穿好高速柴桥出口监控中心大院

2、服务响应及服务人员

服务响应为 7×24 小时，电话响应时间 15 分钟，电话支持无法解决问题的情况下现场到达时间为 1 小时，一般故障修复时间为 4 小时，重大故障须与招标单位协商，尽快解决。

（十）需充放电设备维护

1、维保服务内容

（1）包含充放电设备设备的检测、维护、维修、清洁、防护等。

（2）需提供充放电设备的锂电池更换服务。

（3）对设备进行日常维护时，乙方应遵循甲方的时间安排。日常维护工作结束后需马上提交问题原因及解决报告。

2、服务响应及服务人员

服务响应为 7×24 小时，电话响应时间 15 分钟，电话支持无法解决问题的情况下现场到达时间为 1 小时，一般故障修复时间为 4 小时，重大故障须与招标单位协商，尽快解决。

（十一）路网中心 GQY 大屏延保服务

宁波市公路运输中心路网调度大屏设备主要包括大屏幕投影模块、分布式多屏拼接控制器、高分应用平台及连接线缆等设备组成，是数字公路的基础设施。为确保路网中心数字公路系统的安全稳定运行，要求有专业资质的供应商对上述设备提供保修和维护。

1、服务数量

（1）设备清单

货物设备名称	规格型号	数量	投运年份	品牌
72 英寸高亮 LED 光源投影机	DDW-E1	32	2015	GQY
玻璃屏幕板	72 英寸	32	2015	GQY
分布式多屏拼接控制器	GQY IPW-D100 （4 路 VGA 输入、8 路 DVI 输入、12 路 HDMI 输入、32 路高清视频输入、4 路 4K 输入、32 路 DVI 输出、含高清底图服务器）	1	2015	GQY
控制软件	GQY 亮度自适应控制模块、无线遥控模块及色彩平衡调节软件；DispManage 拼接屏系统管理软件、DispLink 网络高分辨率传输软件	1	2015	GQY
高分应用平台（含多媒体接入、交通综合管理可视化信息）	含超高分辨率 GIS 电子地图快速显示模块、视频监控模块。	1	2015	GQY
72 英寸箱体套件	72 寸反射机箱	32	2015	GQY
底架		8	2015	GQY

2、服务范围

服务对象是宁波市公路路网中心调度大屏设备,主要包括大屏幕投影模块、分布式多屏拼接控制器、高分应用平台及连接线缆等，供应商应对清单中设备进行定期巡检和维护，及时处理设备故障（免费更换和维修故障配件或设备）

3、总体要求

供应商应在充分理解招标文件的基础上，提供完整的投标维保方案，投标维保方案应包括但不限于以下内容：供应商对项目管理及质量控制，检测设备、服务人员组成等。

4、服务内容

（1）大修改造

如设备损坏，须根据所购配件对大屏幕投影模块和图像处理模块进行更换调试，达到产品设计验收要求，按《视频显示系统工程技术规范》（GB50464-2008）标准，采用实地方式验收，由甲方出具服务项目验收证明。

（2）现场保障

在所提供技术服务期限内服务期内派驻现场专职技术人员 1 名提供技术保障及运维服务；

在所提供技术服务期限内应配合用户完成中心相关设备安装、搬运及机房布线等安装、搬运及技术服务工作。

（3）预防性现场巡检维护保养保障

供应商应对服务范围内的系统做定期的现场巡检和维护保养，周期为每月一次，对维保设备的整体运行状态进行评估分析，填写设备巡检报告。重点在于硬件设备及与之相关的各种环境信息、状态的检查，并根据检查结果提供建议，必要时进行预防性维修。逢重大节假日或保供电前期按甲方要求做特殊巡检和维护保养。维护保养的内容至少包括：

投影模块

屏幕清洁；机芯维护；镜头维护；电源模块检查；箱体全面除尘清尘；灯组的检查和清洁；检查投影模块和图像控制器的工作是否正常。

控制器和控制终端

控制器开箱检查；控制器的清洁；控制器硬、软件检测，部件更换；操作控制软件的升级服务和质保服务；控制器和控制终端病毒清理。

投影系统

线缆检查；视频检查；网络检查；投影显示亮度综合检查；系统色彩平衡一致性调整；系统显示图像位置调整，投影模块几何线性调整；检查大屏幕系统的各路信号源使用是否正常；调试大屏幕机械位置和颜色色差；查看大屏幕系统的使用环境；测试易损耗配件的使用情况。

（4）供应商应在投标文件中制定相应的定期维保计划，并按照维保计划及时到甲方现场进行维护保养。

（5）每次定期维护保养结束，供应商应及时提供维护保养报告，详细记录系统诊断过程、操作步骤、必要的系统优化调整建议等。

（6）故障维护

当服务范围内的系统及设备出现故障并向供应商报修时，供应商服务人员应按要求，携带相关检测仪器、备件和材料及时抵达现场进行诊断并排除硬件故障，使系统恢复正常运行，未经许可，供应商不得借助甲方的任何资源。

供应商进行故障排查时，不得发生因对设备的操作导致其他无关设备的异常和故障，或系统故障的进一步扩大。

甲方在使用服务范围内的设备时如遇到问题，随时可以从供应商立刻得到电话支持与帮助。

对于通过电话无法解决的问题，要求供应商服务人员在规定的时间内到达现场服务。如果在现场服务中，由于供应商的技术人员的误操作而导致甲方的系统运行受到影响，供应商将承担全部责任。

所有服务范围内的设备出现硬件故障，供应商均应免费修复或者更换。替换的零部件应按硬件厂商的更换规则进行了必要的升级，以优化用户的系统性能。更换零部件的保修期及保修级别与主设备一致。

每次故障维护结束，供应商应及时提供故障维护报告，详细记录处理过程和结果等，内容包括服务请求、开始时间、结束时间、电话支持内容、现场工作纪要、备件更换情况、故障现象、故障处理方式以及处理结果、设备运行状况等。

甲方系统出现运行问题时，原因可能是多方面的，如操作系统问题、硬件问题、应用软件问题、数据库问题等，基于此原因，供应商应制定多厂家协作支持服务方案，协助甲方迅速诊断，综合解决问题。

（7）整体调优

供应商在做好设备维保工作的同时，应做好系统的整体调优工作，使得系统处于可靠、安全的运行方式，显示画面亮度、色彩和对比度整体均匀，并具有较高的运行效率。供应商负责将设备厂商最新发现的重要问题与 Bug 及时通知甲方，在征得甲方同意后采取相应的防范措施。

（8）故障应急

供应商应在合同生效后一个月内提供设备的应急方案，做好配置文件备份和其它相应的事故预想工作。

（9）培训

供应商应在故障维护的同时，针对性地对故障的现象、分析、诊断、定位等向甲方进行现场指导培训。

（10）服务要求

基本要求

服务期间应遵守甲方的安全制度、保密制度、运维规程，签订保密协议，保证不发生安全事故、泄密事件。

未经甲方同意，供应商不得随意变更服务人员，以及安排常驻服务人员与甲方无关的其它工作。

提供 7×24 小时电话支持，随时接受甲方的技术咨询，帮助甲方迅速解决较容易的、非现场的技术问题。

故障响应要求：在设备故障时，供应商应承诺 7*24 小时服务，在接到故障报修请求后 60 分钟内到达现场，开展故障检测、定位、排除工作（含损坏件更换）。

故障恢复要求：常规的单点或多点故障，在供应商接到故障报修请求后，应于 4 小时内排除故障，恢复正常。特殊故障，如同一故障反复频繁出现等情况，则由供应商制定完整的解决方案，并经过甲方技术负责人确认后，由甲方技术负责人安排合适的时间，通过分阶段排查解决。

供应商服务人员在现场实施过程中所使用的检测设备等应是安全可靠的专用设备，专用笔记本计算机设备应根据维保设备类型预装相应检测软件，放置在甲方现场统一管理。

在服务期结束时，提交运维服务工作总结报告。

维护的主要材料和所需的消耗性材料均由供应商免费提供，且必须为甲方储备充足的易损耗配件，确保甲方大屏幕系统的常年正常运行，并每月对大屏幕机体内外进行清洁工作。

在维保过程中，供应商如果通过维保或者自行检查，发现大屏幕系统仅依靠合同规定的维保已经不能保证安全运行，需要改造、维修或者更换零部件、更新设备时，应当向甲方书面提出，并进行免费改造、维修或者更换零部件、更新设备；发现事故隐患及时告知甲方。

调试维护必须保证质量，确保设备维护后一年内不发生因维护原因造成的设备事故。否则，供应商应当无条件免费返修，返修质量达到符合甲方要求为止。

（11）人员要求

供应商需指定一名主要联系人及两名替补联系人与甲方联系。

供应商指定的现场服务人员应具有专业资质，应将现场服务人员的简历（学历、工作经历）、项目经历（需用户证明）、技能情况、资格证明等在现场备案。

（12）工作要求

建立和完善例行运维手册，根据系统运行状况，建立必要的系统运维监控文档，包括运维规程、运维任务清单、典型运维操作手册等。

建立配置文档，描述系统的组成和结构，建立各系统配置清单，根据系统变更情况及时更新调整系统配置清单。

系统变更维护，根据应用需要，及时调整系统的应用软件及相关技术配置，使系统功能能够满足应用需求，使系统能够保持正常运行。

（十二）其他要求

1、文档管理

乙方需提供本次维保涉及的各类文档、表格，包括但不限于：巡检项目记录表，日常服务报告\故障处理单和部件设备更换单。

2、运维管理

乙方需协助招标单位建立、完善设备运维管理制度及文档，包括但不限于：相关设备的运维操作规程，相关设备及配套软件的日常维护操作文档和故障应急处置方案。同时，要求每季度提交机房运维总体报告，内容包括此季度维保响应次数、时间、人员、内容，备件储备及使用情况，设备健康情况，运维建议等。

3、备品备件

为确保宁波公路运输中心核心机房信息化设备的正常运行，中标单位必须提供备品备件服务，在服务期限内备品备件必须放置在用户处。备件具体要求如下：

备品备件清单

备件类型	备件名称	配置要求	数量	存放地点	品牌要求
网络安全设备	防火墙	百兆防火墙	1	用户机房	国产主流
	安全审计设	日志审计设备	1	用户	国产主流

	备			机房	
	核心交换机	双引擎，配置 24 口千兆电口业务板 2 块，配 48 口千兆电口业务板 1 块，12 口以上千兆 sfp 光口业务板 1 块。	1	用户机房	CISCO/H3C/华为
	交换机	24 口可网管交换机	2	用户机房	CISCO/H3C/华为
	多模模块	万兆 SFP 多模模块	4	用户机房	CISCO/H3C/华为
	单模模块	光模块-SFP-GE-单模模块，1310nm，10KM	4	用户机房	CISCO/H3C/华为
服务器	硬盘	300G SAS 3.5 寸 15K	2	用户机房	联想/HP/DELL
	硬盘	3TB SAS 2.5 寸	2	用户机房	联想/HP/DELL
	电池	495W 电池	2	用户机房	联想/HP/DELL
	电源	750W 电源	2	机房	联想/HP/DELL
存储	硬盘	3.5 寸 600G 15K 存储专用硬盘	4	机房	EMC（vnx 系列）

四、合同金额

本合同总金额为（大写）：_____（¥_____元）人民币。

五、服务期限

本合同期限：_____年____月____日至_____年____月____日；

六、转包或分包

1.本合同范围的服务，应由乙方直接供应，不得转让他人供应；

2.如有转让的分包行为，甲方有权解除合同，追究乙方的违约责任。

七、付款方式

_____

八、违约责任

1.甲方无正当理由拒收接受服务的，甲方向乙方偿付合同款项百分之五作为违约金。

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

3.乙方未能如期提供服务的，每日向甲方支付合同款项的千分之六作为违约金。乙方超过约定日期 10 个工作日仍不能提供服务的，甲方可解除本合同。乙方因未能如期提供服务或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总价 5%的违约金，如造成

甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

九、税费

本合同执行中相关的一切税费均由乙方负担。

十、不可抗力

1.在合同有效期内，因自然灾害等不可抗力因素造成本合同项目经济损失的，甲、乙双方共同协商妥善解决。

2.不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

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

十一、诉讼

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

十二、合同生效及其它

1.合同经双方法定代表人或授权代理人签字并加盖单位公章后生效。服务期满，双方履行合同全部义务，合同价款支付完毕，本合同即告终止。

2.项目采购文件，投标文件视为本合同的组成部分。

3.合同期内乙方履约情况将纳入海曙区综合行政执法局信用等级考评系统。

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

5.本合同未尽事宜，遵照《中华人民共和国民法典》有关条文执行。

6.本合同正本一式贰份，具有同等法律效力，甲乙双方各执壹份；副本陆份，甲乙双方各执叁份。

甲方：

法定代表人或委托代理人：（签字或盖章）

地址：

乙方：

法定代表人或委托代理人：（签字或盖章）

地址：

开户银行：

帐号：

联系人：	联系人：
联系电话：	联系电话：

签约日期：　　年　　月　　日

签订地点：

合同附件：服务满意度月度评分表

服务满意度月度评分表						
姓名		**考评时间**		**考评人**		
考核内容	**考核标准**	**考核计分说明**		**分值**	**得分**	**备注**
日常工作	是否及时响应客户需求	满意 5 一般 4 不满意 3		**5**		
	服务态度是否端正	满意 5 一般 4 不满意 3		**5**		
	是否及时完成工作	满意 5 一般 4 不满意 3		**5**		
应急处理	数据备份情况，制定备份策略并定期进行备份检查	满意 10 一般 9 不满意 8		**10**		
	发生信息化事件后作相关记录，进行报告，并采取积极合理的措施进行处置	满意 10 一般 9 不满意 8		**10**		
环控管理	保证机房温度恒定在 20℃-30℃之间	满意 10 一般 9 不满意 8		**10**		
	保证 UPS 工作正常，电池无漏液	满意 10 一般 9 不满意 8		**10**		
设备管理	交换机，路由器等网络设备的正常运行	满意 10 一般 9 不满意 8		**10**		
	服务器工作是否正常	满意 10 一般 9 不满意 8		**10**		
	及时更换故障硬盘	满意 10 一般 9 不满意 8		**10**		
技术支撑	完成领导与其他单位网络对接的任务，配合软件公司部署服务器等工作	满意 15 一般 14 不满意 13		**15**		
合计				**100**		

注：每月针对服务满意度进行打分，考核总分为 100 分。每月分数不低于 90 分的，合同尾款全额支付；月分数低于 90 分的，每低 1 分，扣除 1 万，最多扣除 12 万元。服务期内累计 3 个月考核低于 90 分的，采购人有权解除合同。

第六章　投标文件格式

自评分表格（做进商务技术文件中）

根据评分标准的表格自行制定自评分表格

一、投标格式

格式一：投标文件的外包装封面格式：

投标文件

项目名称：

项目编号：

标项：/

文件类型：（资格证明文件、商务技术文件、报价文件）

供应商名称：

供应商地址：

开标时启封

年　月　日

2.商务技术文件封面格式：

正本/或副本

投标文件

项目名称：

项目编号：

标项：/

文件类型：（资格证明文件、商务技术文件、报价文件）

供应商名称：

供应商地址：

年　月　日

格式二：有效的企业法人营业执照（或事业法人登记证）、其他组织（个体工商户）的营业执照或者民办非企业单位登记证书复印件（复印件加盖公章）

格式三：提供具有履行合同所必需的设备和专业技术能力的书面声明

具备履行合同所需的设备和专业技术能力的声明

我公司（单位）具备履行合同所需的设备和专业技术能力，具体情况介绍如下：（内容包括：主要设备、专业技术人员、公司资质等）

……..

特此承诺。

供应商（盖章）：

法定代表人或其授权代表（签字或盖章）：

日期：

格式四：提供参加政府采购活动前 3 年内在经营活动中没有重大违法记录的书面声明

近三年在政府采购活动中无重大违法记录的声明

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，特此声明。

供应商（盖章）：

法定代表人或其授权代表（签字或盖章）：

日期：

格式五：供应商资格声明

供应商资格声明函

浙江中创招投标有限公司：

关于你贵司项目（项目编号：　　）的采购公告，本公司（企业）愿意参加采购，并声明：

本公司（企业）具备《中华人民共和国政府采购法》第二十二条资格条件，并已清楚采购文件的要求及有关文件规定。

本公司（企业）的法定代表人或单位负责人与所参加的本采购项目的其他供应商的法定代表人或单位负责人不为同一人且与其他供应商之间不存在直接控股、管理关系。

根据《中华人民共和国政府采购法实施条例》的规定，本公司（企业）如为本采购项目提供项目管理、监理、检测等服务的供应商，不得再参加本项目的采购活动。否则，由此所造成的损失、不良后果及法律责任，一律由我公司（企业）承担。

本公司（企业）具有履行合同所必需的设备和专业技术能力，且本公司（企业）参加政府采购活动前 3 年内在经营活动中没有重大违法记录。否则，由此所造成的损失、不良后果及法律责任，一律由我公司（企业）承担。

本次采购活动中，如有违法、违规、弄虚作假行为，所造成的损失、不良后果及法律责任，一律由我公司（企业）承担。

特此声明！

供应商（盖章）：

法定代表人或其授权代表（签字或盖章）：

日期：

格式六：中小企业声明函格式

中小企业声明函

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. 信息化设备及安全服务外包，属于 其他未列明行业；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、小型企业或微型企业）；

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：

注：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。

格式七：残疾人福利性单位声明函

残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加_____单位的_____项目采购活动提供本单位所需的服务。

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。

供应商名称（并加盖公章）：_____

法定代表人或授权代表（签字或加盖章）：_____

签署日期：_____年_____月_____日

格式八：法定代表人的身份证明

法定代表人身份证明

（法定代表人不参加采购的，此表不用）

供应商名称：

单位性质：

地址：

成立时间：　年　月　日

经营期限：

姓名：　性别：　年龄：　周岁　职务：_

身份证号码：

系（供应商名称）的法定代表人。

特此证明。

供应商：（盖单位公章）

年月日

附法定代表人身份证复印件（正反面）：

格式九：法定代表人授权书

法定代表人授权委托书

（法定代表人参加采购的，此表不用）

致：（采购单位名称）：

我（姓名）系（供应商名称）的法定代表人，现授权委托本单位在职职工（姓名）以我方的名义参加政府采购（项目名称）项目的公开招标活动，代表本公司处理公开招标采购活动中的一切事宜。

我方对被授权人的签名事项负全部责任。

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

被授权人无转委托权，特此委托。

被授权人（签字或盖章）：　　法定代表人（签字或盖章）：

职务：　　职务：

被授权人身份证号码：

供应商公章：

年　月　日

附：法定代表人身份证复印件（正反面）、授权代表身份证复印件（正反面）、授权代表首次开标之日前近三个月供应商所缴纳的社保证明，以上三项内容均须加盖公章。

格式十：供应商基本情况说明

供应商基本情况说明

单位名称			组织机构代码	
注册地址			注册登记号	
经营地址			税务登记证号	
单位性质			注 册 资 本	
经营范围			营业期限	年 月- 年 月
资质情况				
员工数量	共 人，其中，高级职称 人，中级职称 人			
联系电话			传真	
主要业绩				
法定代表人基本情况				
姓名			身份证号码	
职务		职称		学历	
备注：				

兹证明上述声明是真实、正确的，并提供了全部能提供的资料和数据，我们同意遵照贵方要求出示有关证明文件。

供应商（盖章）：

法定代表人或其授权代表（签字或盖章）：

日期：

格式十一：商务条款偏离表

商务条款偏离表

项目名称：

采购编号：

序号	采购文件 的商务条款	投标响应文件 的响应	（偏离）说明
1			
2			
3			
4			
5			
6			
7			
8			

供应商（盖章）：

法定代表人或其授权代表（签字或盖章）：

日期：

格式十二：技术条款偏离表

技术条款偏离表

项目名称：

采购编号：

序号	采购文件 的技术条款	投标响应文件 的响应	（偏离）说明
1			
2			
3			
4			
5			
6			
7			
8			

供应商（盖章）：

法定代表人或其授权代表（签字或盖章）：

日期：

格式十三：类似项目业绩表

类似项目业绩表

项目名称：

采购编号：

序号	项目名称	用户名称	合同金额	合同签订时间	联系人/电话

供应商（盖章）：

法定代表人或其授权代表（签字或盖章）：

日期：

格式十四：项目负责人简历表

项目负责人简历表

姓名		性别		出生年月	
专业		学历		职称	
何时参加工作					
何时进入公司					
从事项目年限					
工作简历					
业主单位	项目名称	规模	合同时间	管理业绩	

供应商（盖章）：

法定代表人或其授权代表（签字或盖章）：

日期：

格式十五：项目人员配置表

项目人员配置表

序号	姓名	性别	职称	专业	联系电话	分工
1						
2						
3						
4						
5						
6						
7						

供应商（盖章）：

法定代表人或其授权代表（签字或盖章）：

日期：

格式十六：备品备件表

备品备件表

备件类型	备件名称	配置要求	数量	存放地点	品牌要求

供应商（盖章）：

法定代表人或其授权代表（签字或盖章）：

日期：

格式十七：投标函格式

投标函

致：（采购单位名称）：

根据贵方为_____项目的采购公告/投标邀请书（项目编号：_____），签字代表（全名）经正式授权并代表供应商（供应商名称）提交标项的投标文件。

据此函，签字代表宣布同意如下：

1.供应商已详细审查全部“采购文件”，包括修改文件（如有的话）以及全部参考资料和有关附件，已经了解我方对于采购文件、采购过程、采购结果有依法进行询问、质疑、投诉的权利及相关渠道和要求。

2.供应商在投标之前已经与贵方进行了充分的沟通，完全理解并接受采购文件的各项规定和要求，对采购文件的合理性、合法性不再有异议。

3.本投标有效期自开标日起_____个日历日。

4.如中标，本投标文件至本项目合同履行完毕止均保持有效，本供应商将按“采购文件”及政府采购法律、法规的规定履行合同责任和义务。

5.已完全明确招标文件中的全部内容，保证按招标文件、投标承诺及政府采购合同要求履行；并在本投标人违反招标文件、投标承诺及政府采购合同时愿意按告知内容接受处罚。

6.供应商同意按照贵方要求提供与投标有关的一切数据或资料。

7.与本投标有关的一切正式往来信函请寄：

地址：_____邮编：_____电话：_____

传真：_____供应商代表姓名_____职务：_____

供应商名称(公章）：_____

开户银行：银行帐号：

授权代表签字：_____日期：_____年___月___日

格式十八：开标一览表

开标一览表

项目编号：

项目名称：　　单位：元

标项号	采购内容	投标报价	服务期	备注
		小写：_____元 大写： 人民币_____元整		
投标声明				

注：报价一经涂改，应在涂改处加盖单位公章或者由法定代表人或授权委托人签字或盖章，否则其投标作无效标处理。

法定代表或授权代表（签字或盖章）：

供 应 商 盖 章：

日 期：

格式十九：投标报价明细表格式

投标报价明细表

（格式仅供参考，可自拟）

项目编号：

项目名称：

金额单位：人民币（元）

序号	名称	细则	单位及数量	单价	金额
投标总价					

法定代表或授权代表（签字或盖章）：
供应商盖章：
日期：

格式二十：商业贿赂行为承诺书

供应商自觉抵制政府采购领域
商业贿赂行为承诺书

致：浙江中创招投标有限公司

开展治理政府采购领域商业贿赂专项工作，是中央确定的治理商业贿赂六个重点领域之一，它既是完善市场经济、构建社会主义和谐社会的客观需要，又是从源头上抑制腐败的有力措施，意义重大、影响深远。为深入贯彻落实中央和省委、省、市、区政府的有关部署及要求，进一步规范政府采购行为，营造公平竞争的政府采购市场环境，维护政府采购制度良好声誉，在参与采购代理机构组织的政府采购活动中，我方庄重承诺：

一、依法参与政府采购活动，遵纪守法，诚信经营，公平竞争。

二、不向采购单位、采购代理机构和政府采购评审专家提供任何形式的商业贿赂；对索取或接受商业贿赂的单位和个人，及时向财政部门和纪检监察机关举报。

三、不以提供虚假资质文件等形式参与政府采购活动，不以虚假材料谋取中标。

四、不采取不正当手段诋毁、排挤其他供应商，与其他参与政府采购活动供应商保持良性的竞争关系。

五、不与采购单位、采购代理机构和政府采购评审专家恶意串通，自觉维护政府采购公平竞争的市场秩序。

六、不与其他供应商串通采取围标、陪标等商业欺诈手段谋取中标，积极维护国家利益、社会公共利益和采购单位的合法权益。

七、严格履行政府采购合同约定义务，不在政府采购合同执行过程中采取降低质量或标准、减少数量、拖延交付时间等方式损害采购单位的利益，并自觉承担违约责任。

八、自觉接受并积极配合财政部门和纪检监察机关依法实施的监督检查，如实反映情况，及时提供有关证明材料。

供应商名称（并加盖公章）：

法定代表人或授权代表（签字或加盖章）：

签署日期：　年　月　日

政府采购活动现场确认声明书

致：采购人

本人经由_____（供应商名称）法人代表（负责人）_____（姓名）合法授权参加信息化设备及安全服务外包项目（采购编号：ZJZC-253055）政府采购活动，经与本单位法人代表（负责人）联系确认，现就有关公平竞争事项郑重声明如下：

一、本单位与采购人之间

□不存在利害关系

□存在下列利害关系：

A.投资关系　　B.行政隶属关系　　C.业务指导关系

D.其他可能影响采购公正的利害关系（如有，请如实说明）_____。

二、现已清楚知道参加本项目采购活动的其他所有供应商名称，本单位

□与其他所有供应商之间均不存在利害关系

□与_____（供应商名称）之间存在下列利害关系：

A.法定代表人或负责人或实际控制人是同一人

B.法定代表人或负责人或实际控制人是夫妻关系

C.法定代表人或负责人或实际控制人是直系血亲关系

D.法定代表人或负责人或实际控制人存在三代以内旁系血亲关系

E.法定代表人或负责人或实际控制人存在近姻亲关系

F.法定代表人或负责人或实际控制人存在股份控制或实际控制关系

G.存在共同直接或间接投资设立子公司、联营企业和合营企业情况

H.存在分级代理或代销关系、同一生产制造商关系、管理关系、重要业务（占主营业务收入50%以上）或重要财务往来关系（如融资）等其他实质性控制关系

I.其他利害关系情况。

三、现已清楚知道并严格遵守政府采购法律法规和现场纪律。

四、我发现_____供应商_____之间存在或可能存在上述第二条第_____项利害关系。

（供应商代表签名）

年　月　日

注：1、本表非投标文件的组成内容，不须在投标文件中提供。
2、本表在开标现场由代理机构提供给各供应商，由各供应商签署。

中小微行业划型标准规定（根据工信部联企业〔2011〕300号制定）

行业	中型企业			小型企业			微型企业		
	从业人员X（人）	营业收入Y（万元）	资产总额Z（万元）	从业人员X（人）	营业收入Y（万元）	资产总额Z（万元）	从业人员X（人）	营业收入Y（万元）	资产总额Z（万元）
1、农林牧渔业		500≤Y＜20000			50≤Y＜500			Y＜50	
2、工业	300≤X＜1000	2000≤Y＜40000		20≤X＜300	300≤Y＜2000		X＜20	Y＜300	
3、建筑业		6000≤Y＜80000	5000≤Z＜80000		300≤Y＜6000	300≤Z＜5000		Y＜300	Z＜300
4、批发业	20≤X＜200	5000≤Y＜40000		5≤X＜20	1000≤Y＜5000		X＜5	Y＜1000	
5、零售业	50≤X＜300	500≤Y＜20000		10≤X＜50	100≤Y＜500		X＜10	Y＜100	
6、交通运输业	300≤X＜1000	3000≤Y＜30000		20≤X＜300	200≤Y＜3000		X＜20	V＜200	
7、仓储业	100≤X＜200	1000≤Y＜30000		20≤X＜100	100≤Y＜1000		X＜20	Y＜100	
8、邮政业	300≤X＜1000	2000≤Y＜30000		20≤X＜300	100≤Y＜2000		X＜20	Y＜100	
9、住宿业	100≤X＜300	2000≤Y＜10000		10≤X＜100	100≤Y＜2000		X＜10	Y＜100	
10、餐饮业	100≤X＜300	2000≤Y＜10000		10≤X＜100	100≤Y＜2000		X＜10	V＜100	
11、信息传输业	100≤X＜2000	1000≤Y＜100000		10≤X＜100	100≤Y＜1000		X＜10	Y＜100	
12、软件和信息技术服务业	100≤X＜300	1000≤Y＜10000		10≤X＜100	50≤Y＜1000		X＜10	Y＜50	
13、房地产开发经营		1000≤Y＜200000	5000≤Z＜10000		100≤Y＜1000	2000≤Z＜5000		Y＜100	Z＜2000
14、物业管理	300≤X＜1000	1000≤Y＜5000		100≤X＜300	500≤Y＜1000		X＜100	Y＜500	
15、租赁和商务服务业	100≤X＜300		8000≤Z＜120000	10≤X＜100		100≤Z＜8000	X＜10		Z＜100
16、其他未列明行业	100≤X＜300			10≤X＜100			X＜10		

说明　1、企业类型的划分以统计部门的统计数据为依据。

2、个体工商户和本规定以外的行业，参照本规定进行划型。

3、本规定的中型企业标准上限即为大型企业标准的下限。