宁波镇海港埠有限公司

2026年-2028年网络安全维护服务项目

招标文件

招标编号：ZS-FW-2026-2

招标人：宁波镇海港埠有限公司

招标代理机构：浙江省成套招标代理有限公司

2026年1月

目　　录

第一章　招标公告

浙江省成套招标代理有限公司受宁波镇海港埠有限公司的委托，拟对宁波镇海港埠有限公司2026年-2028年网络安全维护服务项目进行公开招标，欢迎符合资格条件的投标人前来投标。

一、招标编号

ZS-FW-2026-2

二、本项目采用公开招标，资格后审方式。

三、项目概况

1.项目内容：宁波镇海港埠有限公司2026年-2028年网络安全维护服务，详见第二章 招标需求。

2.服务期限：三年。合同一年一签，根据上一轮合同的履约情况，双方协商一致后可续签下一年度的合同。

3.服务地点：宁波镇海港埠有限公司（招标人指定地点）

4.服务要求：符合技术规格书及合同要求

四、合格投标人的资格要求

1.具有良好的商业信誉和健全的财务会计制度；具有履行合同所必需的设备和专业技术能力。

2、具有合法有效的企业营业执照，且有完成本次招标项目的能力。

3.投标人不得为失信被执行人，招标人对投标人失信信息进行查询（具体以评标当天“信用中国”网站www.creditchina.gov.cn查询为准）。

4.单位负责人为同一人或者存在控股、管理关系的不同单位，不得参加同一标段投标或者未划分标段的同一招标项目投标。

5.本项目不接受联合体投标。

五、招标文件的获取

1.本项目采用电子招标投标方式，投标人可访问浙江省海港集团电子招标采购平台，从浙江省海港集团、宁波舟山港集团网站（http://www.zjseaport.com/jtww/）进入阳光工程-电子招标采购平台后进行投标人注册，并下载“浙江海港投标管家”。本项目招标文件和补充（答疑、澄清）、修改文件均通过“浙江海港投标管家”下载。

2.招标文件下载时间：2026年 月 日 至2026年 月 日16时00分。

3.未取得浙江省海港集团电子招标采购平台数字证书的投标人，投标前应先办理浙江省海港集团电子招标采购平台CA数字证书，具体办理指南及下载链接请至浙江省海港集团电子招标采购平台进行查看。

六、投标保证金

1.金额：**15000元**。

2.投标人应于2026年 月 日16时00分前通过浙江省海港集团电子招标采购平台汇入指定账户。

3.投标保证金应通过**投标单位银行基本账户**汇入，否则视为投标保证金无效。

七、投标截止时间和地点

1.投标文件递交截止时间：2026年 月 日9时00分。

2.投标文件递交方式：

线上递交方式（投标管家工具）：投标人在投标文件递交时间截止前（2026年 月 日9时00分），将电子投标文件加密后递交至电子招标采购平台。

八、开标时间地点及注意事项

本项目将于2026年 月 日9时00分在宁波镇海港埠有限公司综合办公楼A楼A311室在线公开开标。

注意事项：

1. 投标人于投标截止时间之后三十分钟内在“浙江海港投标管家”工具端—进入项目—开标—远程开标模块，点击“确认开标结果”按钮进行确认，如超时未确认，视作投标人已对开标结果确认无误。

2. 本项目采用电子招标，中标单位须在明确中标后、获取中标通知书前将相应的交易服务费缴入平台指定的集团账户（在“投标管家”工具中查看），具体收费标准详见招标文件或平台公告。

九、联系方式

招标人：宁波镇海港埠有限公司

地　址：宁波市镇海区招宝山街道威远路111号

联 系 人：王老师　　联系电话：0574-27694835

投诉受理联系人：葛老师　　联系电话：0574-27683079

招标代理人：浙江省成套招标代理有限公司

地　址：宁波市海曙区翠柏路89号宁波工程学院西校区C栋8楼
联系人：刘晓红、魏超逸、王斌娜、毛宇兰
联系电话：0574-87585597
电子邮件：254497199@qq.com

电子招标采购平台咨询电话：0574-27680520
CA咨询热线：400-666-4230

第二章　招标需求

招标编号：ZS-FW-2026-2

招标人：宁波镇海港埠有限公司

招标代理机构：浙江省成套招标代理有限公司

一、招标内容

项目内容	备 注
宁波镇海港埠有限公司 2026 年-2028 年网络安全维护服务	详见本章三、技术规格书。

二、商务要求

服务期限	三年。合同一年一签，根据上一轮合同的履约情况，双方协商一致后可续签下一年度的合同。
服务地点	宁波镇海港埠有限公司（招标人指定地点）
★付款方式	1、合同签订后 30 天内，招标人凭中标人开具的 50%增值税专用发票（6%税率）支付合同总价的 50％价款。运维服务到期后，甲方确认没有未解决的技术问题后凭中标人开具的 50%增值税专用发票（6%税率）支付合同总价的 50％价款。 2、一次性支付费用在 10 万元以上的，招标人可以不低于 50%承兑汇票的方式支付服务费用。 3、合同价款由招标人通过银行转账方式支付给中标人。
合同签订	本项目最终合同由宁波镇海港埠有限公司与中标单位直接签订。

三、技术规格书

1、项目概述

1.1 项目情况介绍

随着互联网新技术、新应用的快速发展，信息网络已经与国家、组织和个人的行为融为一体、不可分割。各单位的信息安全体系在经历了大规模建设阶段之后，基础网络防护能力明显提升，但安全隐患仍不容忽视。总结最近几年的安全态势，我国信息安全面临的主要安全威胁重点表现在：网站安全事件屡有发生、网站用户信息泄露引发社会高度关注、遭受境外的网络

攻击持续增多、工业控制系统安全事件呈现增长态势、电子政务等应用软件漏洞呈现迅猛增长趋势、针对各级组织的 DDoS 攻击仍然呈现频率高、规模大和转嫁攻击的特点。

为贯彻国家通过安全服务项目，实时掌握宁波市镇海港埠公司系统的网络安全态势，通过终端、流量、日志等方式及时了解宁波市镇海港埠公司安全威胁、风险和隐患，监测其安全漏洞、僵木蠕毒传播和网络攻击情况；形成网络安全监测预警处置工作机制。逐步实现从“基于威胁的被动保护”向“基于风险的主动防控”转变，为数字化转型保驾护航。

2、安全技术服务及工具要求

2.1 网络安全服务

序号	品类	产品名称	描述	数量	备注
1	**安全服务**	资产持续梳理评估	使用绿盟科技的远程漏洞评估产品，检测网络设备、操作系统、数据库和应用服务中存在的安全漏洞及配置并进行资产发现梳理服务，给出相关建议。	8 周	
		渗透测试	通过人工黑盒的测试方式，发现网络和业务系统中存在的安全缺陷，提供复测、渗透测试报告和漏洞修复建议。	4 次/年	
2	**一体化安全运营服务（MDR 服务）**	资产管理服务	安全运营工程师到客户现场，基于绿盟安全运营平台，提供周期性资产核查及资产变更管理服务。	每季度一次	
		脆弱性验证及管理服务	到客户现场提供周期性漏洞扫描或渗透测试，针对中高危漏洞进行准确性验证并给出验证结果，实现漏洞生命周期管理。	每季度一次	
		7*24 远程威胁监测及分析响应服务	绿盟远程运营专家团队，为客户提供 7*24 小时的威胁事件监测及分析服务，并提供处置建议。对常见网络安全事件(挖矿、勒索、蠕虫、入侵等)进行快速响应处置，包括对事件进行预判定性、分析排查、提供遏制方案限制影响扩大、提供清除和修复建议并出具应急响应报告。	一年	
3	**网络及系统安全服务**	持续对资产及业务梳理服务	对生产和办公网终端资产进行持续梳理，对生产和办公网络设备资产进行持续梳理，对生产和办公网安全策略梳理和细化，并提供详细的资产梳理和安全策略梳理记录。	一年	
		安全架构设计与优化服务	帮助企业设计和优化其安全架构，以更有效地防御网络攻击和威胁。	一年	
		服务器系统漏洞加固及业务安全优化服务	服务器系统加固，对生产及办公网服务器系统漏洞的安全加固。 提供生产和办公网业务系统的安全加固建议，以及协助梳理业务及增强安全防护策略。	一年	

		网络安全技术防护策略持续改进服务	帮助企业制定或优化其网络安全策略和操作流程。 实时对安全设备进行日志监控，在设备发现异常行为时，及时通过黑名单、访问控制列表等方式进行拦截处理施。 对安全监测和安全风险检查的结果进行综合分析研判，识别网络安全风险、脆弱性和不合规配置项，从整体网络安全技术防护策略的角度提出准确、有效的改进措施，协助开展策略配置调优，以持续提升安全运行和防护能力。	一年	
		人员技能安全培训服务	为企业员工提供网络安全意识和最佳实践的培训，增强对钓鱼攻击、恶意软件等威胁的识别能力。	一年 2 次	
		合规性评估和咨询	针对行业特定的安全合规要求（如等保 2.0 合规要求），提供合规性评估和改进建议。	一年 2 次	
		重保期间的安全防护服务	针对重要节假日或重要时期的安全保障服务： 增强网络监控：在重保期间加强网络监控，以便及时发现和响应异常活动或攻击。 强化防御措施：提前更新安全系统，如防火墙、入侵检测系统和恶意软件防护，确保所有防御措施都是最新的。 应急准备和响应计划：确保有一个详尽的应急响应计划，并在重保前进行复习和更新。确保关键人员了解他们在应对潜在安全事件中的角色和责任。 备份和数据恢复：在重保期间前确保所有关键安全设备的配置数据都已备份，并验证恢复流程的有效性。 限制访问控制：重保期间可能需要实施更严格的访问控制措施，特别是对于关键系统和数据。 协调沟通：确保安全团队和关键决策者可以在需要时迅速沟通和协调。 审计和合规性检查：进行定期的安全审计，确保符合所有相关法律、法规和行业标准。 灵活调整策略：根据当前的威胁情报和组织的特定需求，灵活调整安全策略和措施。	15 天/年	
		安全事件应急响应处理服务	在发现信息安全威胁后第一时间进行跟进处理，最大限度的降低安全事故带来的危害，减少安全事故带来的影响，将安全损失降到最低； 当入侵或者破坏发生时，对应的处理方法主要的原则是首先保护或恢复计算机、网络服务的正常工作；	一年	

			然后再对入侵者进行追查，并对整个应急响应过程进行记录。对于紧急事件响应服务主要包括准备、识别事件（判定安全事件类型）、抑制（缩小事件的影响范围）、解决问题、恢复以及后续跟踪。		
		常规网络安全维护服务	安全服务期内，提供以下维护保障：	一年	
			为信息化系统内各个应用系统提供常规维护服务		
			成立技术小组提供 7*24*2 小时技术支持服务		
			提供 7*24 小时服务热线电话，随时响应用户的咨询		
			制定各项业务系统优化策略，保障信息化系统健康稳定运行		
		安全设备运行状态巡视服务	1）每季度 1 次安排安全工程师对生产和办公网涵盖的安全设备进行详细监控检查	一年	
			2）按照计划安排安全工程师对相应系统进行安全巡检并做好记录与总结		
			3）在巡视时如发现设备和系统异常，及时通知相关人员和产品售后服务中心，进行故障处理		
4	**主机安全防护**	EDR 终端安全	绿盟主机安全防护系统许可 20 个 license	1	
5	**堡垒机运维审计**	堡垒机（运维审计）	100 个绿盟堡垒机设备授权(主备堡垒机各 50 个 license)	1	

2.2 服务工具要求

2.2.1 安全管理平台

技术指标	指标详细要求
数据采集	平台应基于大数据基础构架，具备海量数据接入、存储、访问、计算能力。
	平台应支持内置 900+设备日志解析规则查看以及筛选，包括但不限于网络设备（防火墙、交换机、网关）、安全设备（入侵检测设备、WEB 攻击防护设备、APT 检测设备、防火墙、网络审计、流量探针等）、终端主机日志、数据库等。
	平台应支持 ipv4\ipv6、多种协议的数据接入，包括但不限于 FTP、SFTP、UDP、TCP、Netflow、本地文件系统、KAFKA、JDBC/ODBC。
	平台应支持界面化配置规范化规则采集第三方日志实现异构日志格式归一化。解析规则支持正则表达式等前置过滤方式及 json、kv、csv、正则表达式类型的解析规则，支持界面划取字段配置、多级解析提取嵌套字段、配置规范化规则对解析提取的字段进行字段类型、名称、取值规范化。
	平台应支持针对采集日志配置数据清洗规则以过滤无业务价值数据。

威胁检测与分析	平台应支持多源异构安全设备、网络设备、全流量设备、终端设备、APT 威胁检测设备、漏洞扫描设备、网站安全检测、VPN 设备等数据接入与威胁分析，输出可疑威胁事件。
	平台应支持规则分析能力，应支持不少于 700 种内置分析识别规则并支持内置规则的升级，支持用户自定义规则，用户自定义规则可以支持导入导出。
	平台应支持复杂模型的分析能力，应支持 DGA、决策树机器学习算法，提供僵尸网络场景、隐蔽信道场景、WebShell 场景的检测，并输出相关的可疑事件。
	平台应支持原始日志的查询分析能力，支持提供快捷的全文检索条件，也支持通过时间范围、IP 地址、日志类型、来源设备等条件进行查询，并对查询结果提供按时间分段的统计图，查询结果支持列表形式进行展示，支持自定义列表中展示的列，查询结果支持导出为 Excel 文件。
	平台应支持安全事件的查询分析能力，支持提供快捷的全文检索条件，也支持通过时间范围、IP 地址、事件类型、来源设备、威胁等级等条件进行查询， 并对查询结果提供按时间分段的统计图，查询结果以列表形式进行展示，支持自定义列表中展示的列，查询结果支持导出为 Excel 文件。支持在页面内展示事件详细信息，事件详情包括但不限于：事件摘要、事件关键属性，攻击过程，涉及的攻击者、受害者详情，还包括关联的日志信息、情报信息，并展示攻击者使用的 ATT&CK 中定义的战术及技术。
	平台应支持基于资产维度的风险资产视角分析，支持展示失陷主机、高风险主机、低风险主机，支持总数/今日新增数/已处置数，支持风险资产组 Top5/Top10 展示，支持今天/近 7 天/近 30 天的数据展示切换，支持资产列表展示，支持主机 IP、主机名等多种条件进行查询，查询结果支持导出为 Excel 文件，支持自定义列表中展示的列，支持资产列表中跳转到一键响应/加入白名单/变更状态/详情，支持基于资产组/业务视图/组织架构进行风险资产统计分析。
	平台应支持简易模式的自定义规则，可支持用户在选择日志类型、设置常见日志类型字段过滤条件之后，即可新建或编辑规则，从而生成事件。
	平台应支持专家模式的自定义规则，可支持行为分析、多源关联分析、机器学习等多种分析模式，同时可按需自定义生成的事件模版信息如威胁等级、攻击链阶段、事件类型、攻击意图等。
	平台应支持主机、应用等弱口令访问行为的检测，弱密码应加密展示且需要管理员的二次独立认证授权后方可查阅明文弱口令。同时支持批量导出弱口令帐号能力以便于弱口令帐号的分发整改。
	平台应支持网络代理软件、自由门软件、无界软件等代理翻墙风险行为的检测。
	平台应支持远程控制控制风险行为的检测，如向日葵、TeamViewer、远程连接 windows 命令行、远程控制工具等。
	平台应支持 POP3、IMAP、SMTP、FTP、TELNET 应用帐号的异地登录风险行为检测。
	平台应支持对重点事件的标记监控以及对重点事件的攻击结果进行判断，判断攻击成功/失败/未确定。
	平台应支持基于全流量数据进行流量纬度的可视化统计，包括流量趋势、应用分布、主机流量、端口访问、境外访问、主机外联、域名访问、DNS 请求、高频访问页面、低频访问 TOP 10。
资产管理	平台应支持多维度资产管理，进行多维度资产视图分析，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。
	平台应支持资产发现能力，至少具备主动扫描发现资产能力，主动扫描支持联动漏扫设备下发资产扫描策略并上报扫描结果。**（提供功能截图并加盖投标人**

	公章）
	平台应支持围绕客户的资产树展开风险分析。通过基于资产树的方式对资产进行脆弱性呈现，通过资产数能够快速了解出现高危脆弱性的资产所处位置、所属单位（部门）、负责人等，从而快速定位、快速解决。
漏洞管理	平台应支持对重点系统或重点网站的漏洞扫描能力，平台支持向安全采集探针下发系统漏洞扫描任务、网站安全漏洞扫描任务、口令猜测扫描任务，通过平台进行统一扫描任务监控、管理，对扫描结果可以进行可视化呈现。
	平台应支持在线下发漏洞扫描任务的能力，应支持灵活的任务策略配置，包括但不限于：调度策略（立即、定时、周期）、扫描设备选择（支持自动/手动指定扫描设备进行漏洞扫描）、漏洞模板策略、登录扫描参数、扫描引擎参数等。
	平台应支持漏洞闭环分析可视化展示，包括脆弱性值、脆弱性等级分布、漏洞数趋势、脆弱性值趋势、漏洞类型分布、漏洞 TOP、资产脆弱性 TOP 等。
	平台应支持漏洞报表功能，可选择生成资产风险报表、系统扫描报表、网站扫描报表、漏洞处置报表、配置核查报表等，为客户撰写安全分析报告提供支撑。
情报分析	平台应支持接入威胁情报，支持在线自动接入和离线手动导入。
	平台应支持多种类型的情报接入，至少包含：ip、url、域名、样本、漏洞、热点事件情报。
	平台应支持接入热点事件情报，热点事件情报至少包含：事件名称、事件描述、首次发现时间、最近更新时间、关联的 ip 列表、关联的 url 列表、关联的域名列表、关联的样本列表、关联的漏洞列表、其他关联情报信息。
	平台应支持自动对安全事件、资产进行情报匹配，支持展示不同类型情报匹配中事件的历史趋势、各类型情报命中事件 top 条目、攻击链各阶段命中情报事件数目、命中情报事件攻击类型分布、命中情报事件威胁级别分布、高中低各级别漏洞情报匹配资产数目、关联资产数目漏洞情报 top 条目，对于匹配中情报的事件、资产，能够在相应列表或详情界面下钻到匹配中的情报详情。
	平台应支持界面查看热点事件情报以及配置热点情报预警预警，支持界面配置关心的情报关键词和预警邮箱，当收到事件情报更新时自动匹配关键词，如果匹配中，触发预警发送邮件。
态势呈现	平台应支持所监测网络安全情况的态势呈现能力，态势呈现包括但不限于综合态势、威胁态势、脆弱性态势、环境感知态势、运维响应态势。**（提供功能截图并加盖投标人公章）**
	平台应支持对网络内外部威胁态势感知与可视化呈现，包括但不限于外部攻击与外部攻击类型 TOP、内部攻击类型 TOP、行为分析机器学习以及多源分析的威胁感知事件数、僵木蠕态势的详细分布、网络入侵事件分布、网站安全事件分布以及 APT 攻击事件 TOP 等。
	平台应支持对网络环境中各元素多方位的态势感知与可视化呈现，包括但不限于资产数量、失陷资产数、业务访问 TOP、端口开放端口 TOP、应用分布 TOP、协议分布 TOP、外联国家 TOP、设备类型分布、风险帐号 TOP 及告警来源 TOP 等。
安全治理	平台应支持态势大屏轮播，支持轮播时长设置，支持轮播顺序和数量调整，支持大屏上增加客户 logo、大屏名称自定义，支持安全事件/风险资产可配置大屏弹窗和声音告警，支持大屏默认展示省级地图设置。**（提供功能截图并加盖投标人公章）**
	平台应支持安全态势指标展示，安全态势指标应至少包含威胁指标、隐患指标、事件指标等，支持通过加权计算得到综合指标值。

事件运维与监控	平台应支持对威胁、失陷主机、漏洞等事件进行统一运维处理，提供统一入口。
	平台应支持最近 1 小时、24 小时、7 天的全局运维事件统计与监控并可按需自定义仪表盘，监控内容包括但不限于各类统计数据如事件、失陷资产、日志、攻击源、情报等，支持重点事件、风险处置监控、攻击源、事件类型、外发事件类型 TOP 等统计监控，支持资产威胁类型、资产发现、高危资产、资产脆弱性 TOP 等统计监控；支持漏洞、网站监测事件、脆弱性资产 TOP 等统计监控。
	平台应支持工单数据的权限管理，所有的运维人员都可查看平台所有工单，可通过责任人是自己来查看自己的工单;仅支持对责任人是自己账号的工单进行操作。
一键封堵	平台应支持针对 IP、域名、会话进行封堵，支持主机隔离、流量牵引等方式联动设备进行封堵，设备类型包括但不限于防火墙、WEB 应用防火墙、网络流量探针等。
	平台应支持封堵状态获取及查看，支持判断封堵成功、封堵失败、解封成功、解封失败等状态。**（提供功能截图并加盖投标人公章）**
	平台应支持对被封堵对象的解封能力，支持配置解封时间，到期自动解除封堵。
应用场景	可以应用在等保合规、日志审计、攻击检测、响应处置、资产发现、漏洞管理、情报预警、态势感知、安全运营、安全报表等场景使用。
其他	中标后七个工作日内，提供样机进行上述功能要求的逐一测试验证，测试中发现虚假应标的行为将取消中标资格并保留追究相关责任的权利。

2.2.2 攻击流量分析系统

技术指标	指标详细要求
品牌	★必须与原有态势感知安全管理平台同品牌（绿盟）。
部署模式	旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响。
流量采集	支持对 DNS、HTTP、FTP、SMTP、POP3、IMAP、SMB、Telnet、LDAP、MYSQL、ORACLE、MSSQL、PG、SSL、TLS、QQ、TCP、UDP、ICMP、SMB、WEBMail 等常见协议的深度解析和还原。
	支持流量灰名单，关注重点资产流量，对命中灰名单的流量进行流量还原和威胁检测。灰名单类型包括 IP、端口、IP+端口。
资产发现	支持从流量中自动识别资产信息和归类，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。支持人工录入资产维护整体资产库，并支持增删改查。
文件还原	支持对流量中出现的文件进行发现和还原，支持还原的协议包括：HTTP、FTP、SMTP、POP3、IMAP、SAMBA、WEBMAIL。
流量存储	支持对威胁相关的数据包进行存储，供关联分析和取证使用。
	支持对流量中检测到的恶意文件进行存储，供关联分析和取证使用。
	支持对实时流量采集的 pcap 包进行全量存储，供追溯分析和取证使用。**（提供功能截图并加盖投标人公章）**
	支持对深度解析的协议进行存储，存储日志类型至少包括：会话日志、HTTP

技术指标	指标详细要求
	日志、EMAIL 日志、TELNET 日志、认证日志、数据库日志、登录日志、SSL&TLS 日志、FTP 日志、DNS 日志、ICMP 日志、文件还原日志、社会账号日志、5G 日志。
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 9000 种以上。
	支持多种抗逃逸攻击检测，检测类型包括：PDF 漏洞利用规避攻击、 Adobe PDF JavaScript 文件规避攻击、Metasploit PDF 漏洞利用规避攻击。
WEB 应用检测	支持针对主流 Web 服务器及插件的已知漏洞攻击检测。Web 服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS 等；插件应覆盖：dedecms、phpmuadmin、PHPWind、shopex、discuz、echsop、vbulletin、wordpress 等。
	支持对 sql 注入、XSS、SSI 指令、Webshell、目录遍历、远程文件包含等网络攻击检测。
	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。
高级检测	支持传输安全检测日志，包括网络攻击检测日志、漏洞利用攻击检测日志、僵尸网络检测日志、业务弱点发现日志。
	支持传输访问检测日志，包括正常访问、风险访问、违规访问。
	内置恶意文件静态检测引擎，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
违规访问检测	▲支持隐蔽隧道检测，检测企图绕过防护的 ICMP/DNS 隐蔽通信隧道，发现 C&C 通信。**（提供功能截图并加盖投标人公章）**
特征库	内置 URL 库、IPS 漏洞特征识别库、应用识别库、WEB 应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库。
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。
管理功能	支持设备内置简单命令行管理窗口，便于基础运维调试； 可实时监控设备的 CPU、内存、存储空间使用情况； 能够监控监听接口的实时流量情况。
部署	支持多台采集器同时部署于采购人网络不同位置并将数据传输到同一套分析平台。
其他	中标后七个工作日内，提供样机进行上述功能要求的逐一测试验证，测试中发现虚假应标的行为将取消中标资格并保留追究相关责任的权利。

2.2.3 资产漏洞评估系统

技术指标	指标详细要求
漏洞管理和分析	检测的漏洞数大于 240000 条，兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准。

	产品支持对系统漏洞扫描、web 漏洞、配置合规进行检查和综合分析，可输出同时包含漏洞扫描和配置核查结果的报表。
	支持提供高级漏洞模板过滤器，将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中。
	内置不同的漏洞模板针对 Unix、Windows 操作系统、网络设备和防火墙等模板，同时支持用户自定义扫描范围和扫描策略；自动模板匹配技术。
	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，提供详细漏洞列表。
	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 5000 条相关漏洞。
	支持扫描物联网设备的漏洞，需覆盖常见品牌摄像头、打印机、路由器，摄像头需能扫描海康威视、宇视、大华、亚安、派尔高，打印机需能扫描惠普、三星，路由器需能扫描 TP-LINK、D-LINK、NETGEAR。
	支持扫描容器镜像存在的漏洞，能扫描互联网上公开仓库中的镜像以及私有仓库中的镜像。
	支持对 C/C++/Python/Java/Php/go 等语言的代码解析，语言的词法、语法分析。内置缺陷模板和缺陷规则，并可以自定义。
	支持对扫描出的漏洞提供取证性质的验证并输出报告，直观展示漏洞利用过程和危害性
	支持通过在目标资产部署终端代理 agent 方式，实时精准获取资产信息，进一步完成漏洞分析扫描。
	▲支持专门针对 DNS 服务的安全漏洞检测，包括 DNS 投毒等漏洞检测能力；支持“幽灵木马”检测。**（提供功能截图并加盖投标人公章）**
	支持断点续扫，可对已完成的扫描任务中没有被覆盖到的目标重新下发扫描任务。
	支持扫描时间段控制，只在指定时间段内执行任务，未完成任务在下一时间段自动继续执行。
	支持复用已有任务配置用于新的扫描任务。
	支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态。
风险展示和报表	▲支持通过仪表盘直观展示资产风险值、主机风险等级分布、资产风险趋势、资产风险分布趋势等内容，并可查看详情。**（提供功能截图并加盖投标人公章）**
	支持高级数据分析，可对同一 IP 的两次扫描结果进行风险对比分析，并可在线查看同一 IP 的多次历史扫描结果。
	支持显示扫描结果，包括扫描进度、主机存活数、预计扫描时间、漏洞风险信息等。

	报表能提供针对不同角色的默认模板，离线报告支持 HTML、WORD、EXCEL、PDF 等格式,报告可以直接下载或自动通过邮件直接发送给相应管理人员。
	提供灵活的报表自定义，可定制报表标题、封面 logo、报表页眉和页脚、报表各章节显示内容。
其他	中标后七个工作日内，提供样机进行上述功能要求的逐一测试验证，测试中发现虚假应标的行为将取消中标资格并保留追究相关责任的权利。

2.2.4 绿盟主机安全防护

指标	**产品功能参数**
授权点位	绿盟主机安全防护系统的许可 20 个 license，并提供一年原厂服务。 **★须提供原厂针对该项目的服务承诺函。**
操作系统适配	要求支持多种操作系统，包括但不限于 RHEL/CentOS 6 32/64 位、RHEL/CentOS 7 32/64 位、Ubuntu、Debian、Suse、SunOS5.10、Windows 7 及以上、Windows Server 2003 及以上、中标麒麟、银河麒麟、UOS、Kali GNU/Linux 2020.1 x64 server、MacOS 等操作系统。
安装部署要求	支持客户端静默安装，无感知运行，可配合桌管等工具推送至全网。
	支持客户端自动升级、灰度发布等升级方式，可配置灰度发布地址。
客户端资源占用	要求客户端对终端系统 CPU 占用低于 2%，内存占用低于 200M，终端软件不大于 1M。内置客户端资源监控机制，保证终端业务正常运行。
终端自我保护	支持客户端自定义设置或采取随机方式命名服务，以隐藏自身。
	要求客户端支持防卸载功能，用户需要提供卸载密码才能卸载客户端。
终端安全态势	支持整体终端安全态势分析及可视化展示，包括攻击链统计、网络访问统计、威胁事件类型统计、攻击诱捕统计、弱点统计、事件列表、事件趋势统计等，支持系统整体评分，接入容量占比和月事件总数等。
终端统一管理	支持对接入终端包括 PC、服务器、云主机等进行统一管理，可根据业务需求对终端进行资产分组。
	支持对指定终端上的客户端软件进行更新、禁用、卸载等操作，对已识别风险的主机一键隔离。
	通过自定义模板的方式可对指定终端或资产组进行安全防护策略配置。
	对安装了违规软件的主机，能够向主机推送警告或提示消息，能够编辑消息标题和内容。
资产清点	支持从终端和资产两个维度对全网资产进行统一清点以及展示，清点资产包括软件应用、WEB 服务、WEB 站点、数据库、中间件、网络访问等。
	支持采集汇总终端上安装的应用软件信息，终端软件安装情况能够进行全局汇总，支持使用关键词进行全局检索。
一键安检	按主机合规要求，可对全网主机执行一键合规检查，快速完成合规安检信息汇总，检查项包括但不限于主机名设置合规、防火墙合规、系统更新合规、屏保合规、共享合规、加密盘合规、杀毒合规、浏览器合规、wifi 共享合规等。
合规结果查询	要求提供终端用户侧的自检方式以及合规结果查询。
终端漏洞发现	具备漏洞发现引擎，无需要远程扫描，即可发现终端资产存在漏洞；支持展示漏洞 TOP 与漏洞分布情况，进行漏洞评估，展示漏洞情况和列表，并

	能以漏洞视角查询命中的终端。
漏洞库数量	漏洞库兼容 CVE、CNVD、CNNVD，漏洞数量大于 22 万。
弱口令分析	支持本地弱口令识别，支持 Windows、Linux 系统，默认提供 100 万量级密码字典。
病毒查杀	支持内置轻量级病毒检测引擎，提供最新的热门和易攻击的病毒特征，方便快速查杀电脑关键位置及运行中的文件进程。
威胁事件识别	支持内置终端攻击事件分析能力，能够识别威胁事件作，包括：APT 攻击、勒索病毒、挖矿、蠕虫木马、感染型病毒、恶意程序、黑客程序、钓鱼、漏洞利用程序、黑名单进程等。
风险行为识别	支持内置终端风险行为识别能力，能够识别风险行为，包括系统网络嗅探、暴力破解、漏洞利用、提权、绕过身份验证、可疑命令/任务/进程/脚本执行、可疑凭证获取、可疑权限控制、可疑日志清理行为、可疑文件操作行为、系统高危命令、可疑远程操作行为、异常进程创建行为、异常用户操作行为、可疑 USB 操作行为、创建或加载自启动风险项、零信任登录失败等。
webshell 检测	支持对 php，jsp，aps 的文件进行 webshell 检测。
powershell 检测	检测利用 powershell 执行恶意操作，包括账号密码暴力破解、提权、修改注册表、监控敏感信息、执行恶意命令等。
反弹 shell 检测	通过对用户进程行为进行实时监控，结合父子进程链及进程通信行为分析，从攻击本质特征入手及时发现反弹 Shell 行为，并在告警中详细展示进程树及远控 ip 等信息。目前已识别支持的类型包括：bash 反弹、curl、wget、netcat 各类命令反弹、脚本反弹、应用服务反弹等。
钓鱼攻击检测	采用动态执行和静态文件两种检测方式有效应对钓鱼攻击行为并生成告警。
防勒索病毒	通过威胁诱捕技术、终端异常行为分析和特征值匹配的多重检测机制，可有效检测已知和未知勒索病毒，并快速对其进行阻断。
威胁规则库	威胁规则库可单独升级，默认支持上百条行为规则（不含病毒库）。
终端隔离	提供一键响应操作，支持对终端风险的快速隔离，和访问的阻断控制。
一键响应	全面封锁隔离能力，包括主机隔离、网络链路封禁、文件隔离、进程查杀等。
网络微隔离	提供统一的访问控制策略设置，可配置访问控制，实现主机侧南北向、东西向细粒度的按需访问控制。
快速任务	支持通过自定义检测模板对主机进行一键任务下发，应对 0day 漏洞等快速应急响应场景；提供多种内置用例包括但不限于指定文件查询、远程代码漏洞检测、webshell 恶意扫描样本工具等。
情报分析	支持接入多种类型的威胁情报，包括 IP、域名、样本 hash；平台应支持自动对安全日志、事件进行情报匹配，支持展示不同类型情报匹配中事件的趋势、各类型情报命中事件 top 条目、命中情报事件攻击类型分布、命中情报事件威胁级别分布，对于匹配中情报的事件，能够在相应列表或详情界面下钻到匹配中的情报详。
事件识别分析	▲集中统计分析和展示识别到的攻击事件；支持安全事件的查询分析能力，支持提供快捷的全文检索条件，也支持通过时间范围、IP 地址、事件类型、来源设备、威胁等级、情报命中等条件进行查询， 并对查询结果提供按时间分段的统计图，查询结果以列表形式进行展示；支持在页面内展示事件详细信息，事件详情包括但不限于：事件摘要、事件关键属性，攻击过程，涉及的攻击者、受害者详情，还包括关联的日志信息、情报信

	息，并展示攻击者使用的 ATT&CK 中定义的战术及技术，以及基于攻击流程展示各项攻击技术之间的关联路径。**（提供功能截图并加盖投标人公章）**
风险进程分析	支持对风险事件内进程的父子调用关系进行可视化呈现，可追溯恶意进程关联的文件、网络等关键证据，协助安全运维人员判断是否为恶意进程，并提供快速处置手段。
取证分析能力	支持提供取证分析能力，支持取证日志快速检索分析能力；用户可查看终端所采集的所有原始日志、指纹信息等，可按日志类型、IP 等过滤条件进行筛选。
规则自定义能力	▲用户可自定按日志内容进行配置攻击识别检测规则。**（提供功能截图并加盖投标人公章）**
诱捕能力	终端侧提供系统、网站、数据库等服务模拟，进程、文件、漏洞模拟等诱捕能力，至少包括 tcp、ssh、telnet、http、ftp、rdp、mysql、postgres、sftp、samba、tomcat 等。
诱捕设置	提供诱捕策略配置，提供选择设陷的终端筛选条件配置，控制条件设置。
深度仿真	提供隔离的仿真环境沙箱，部署诱捕环境，并感知采集诱捕事件，支持对蜜罐事件、攻击进程，攻击关系，注入的模块等信息进行可视化呈现。
报表导出	支持按条件对全网终端资产信息、采集的终端原始日志、异常告警等进行报表导出。
运维监控	支持实时监控当前系统运行总资源使用情况和当前组件运行情况，当前系统运行总资源使用情况包括内存、CPU、磁盘使用率和 IO、网络 IO、负载、HA 状态等，当前组件运行状态包括 Zookeeper、Hadoop、Kafka、Elasticsearch、Spark 等。
安全运营平台联动	▲支持与态势感知安全管理平台进行联动，上报终端日志及事件以及执行平台下发的一键封堵指令。
其他	中标后七个工作日内，提供样机进行上述功能要求的逐一测试验证，测试中发现虚假应标的行为将取消中标资格并保留追究相关责任的权利。

2.2.5 绿盟堡垒机运维审计

类别	参数	功能与技术描述
配置要求	**授权点数**	绿盟堡垒机 100 个 license(主备堡垒机各 50 个 license)，并提供一年原厂服务。 **★须提供原厂针对该项目的服务承诺函。**
用户权限管控要求	**三权分立**	系统默认自带三权分立用户，系统管理员、运维管理员和审计管理员权限相互制约，缺省用户账号密码遗失后仅能被重置。
	系统状态和信息展示	支持向管理员展示系统标识、运行时间、资源状态、网络状态、版本等系统关键信息。
	运维概要展示	支持向运维管理员展示全局运维概要信息、包括运维人员总数、当前在线会话数量、所有设备总数、24 小时内设备运维趋势图、运维会话统计表、一周内运维 TOP10 统计表等。
	访问授权	除用户身份认证外，对特定目标设备访问、对特定命令的执行还需要高级管理员授权才能访问。授权审批方式支持 web 审批。
	混合认证	用户登录堡垒机支持多种认证方式，包括本地静态密码认证、LDAP 认证、RADIUS 认证、证书认证、USBKEY 认证、短信认证等身份认证方式；支持可知因素和不可知因素的双因素认证；其中证书认证支持国密算

		法。
托管设备管理要求	**批量操作托管设备**	支持批量导入/导出目标设备信息；可批量修改设备类型、IP、部门、登录方式、会话空闲时间等属性信息。
	幽灵账号发现	支持管理员自定义幽灵账号开启和关闭。
		支持自动发现运维人员运维过程中创建的后门账号行为，并以列表方式向设备管理员展示托管设备中所有的后门账号信息。
	孤儿账号发现	支持管理员自定义孤儿账号开启和关闭。
		支持自动发现运维人员离职后遗留不用孤儿账号，并以列表方式向管理员展示托管设备中所有的僵尸账号，支持自定义未使用天数。
	孤儿设备发现	支持自动发现托管设备中长时间不被运维的僵尸设备，并以列表方式向管理员展示孤儿设备，支持自定义未访问天数。
	▲设备自动发现	支持自动发现指定网络中存活的设备，并自动添加到系统中进行托管。**（提供功能截图并加盖投标人公章）**
	设备账号改密审批	设备账号改密执行需要双人操作执行，一人配置改密，一人审批改密。
运维审计功能要求	**支持多种方式访问托管设备**	自动登录目标设备：运维人员不必知道目标设备帐号及密码，无需进行二次登录认证，实现单点登录。
		支持 WEB 调用本地客户端程序，如 putty,securecrt,xshell,winscp,xftp,mstsc 等客户端单点登录堡垒机运维目标设备。单点登录器不会被安全软件提示存在风险。
		▲支持本地文件客户端程序，如 winscp,xftp 等客户端直接访问堡垒机选取托管设备进行运维，提供技术优势证明材料。**（提供功能截图并加盖投标人公章）**
	运维实时监控	支持实时监控通过 SSH、SFTP、RDP、VNC 、Telnet、FTP、X11 等协议的操作行为；对监控到的非法操作，可实时手工切断。
	操作行为记录	Telnet、SSH 审计内容：包括访问起始和终止时间、用户名、用户 IP 地址、目标设备 IP、设备名称、协议类型、事件等级及操作内容回放。
		RDP、VNC 协议审计内容：包括访问起始和终止时间、用户名、用户 IP 地址、目标设备 IP、设备名称、协议/应用类型、事件等级、操作内容等；支持操作内容录像回放。
	综合审计报表	堡垒机可以按时间、运维协议类型、指定用户、指定设备及各类子报表类型定制报表，报表支持 Word、excel 格式导出； 报表标题可自定义。
	图形运维管控	支持可通过参数配置开启或关闭图形协议运维行为录屏审计，但不影响图形协议会话审计。以便满足客户防范涉密运维行为泄露。**（提供功能截图并加盖投标人公章）**
		支持对全部或个别用户 RDP 协议运维时磁盘映射功能使用的开启和关闭控制，即用户 A 对设备 1 运维可使用磁盘映射功能，而用户 B 对设备 1 运维不可使用磁盘映射功能。
	文件运维管控	文件上传、下载文件、删除文件、新建文件夹、删除文件夹和重命名文件/文件夹行为控制。
		支持可通过参数配置开启或关闭文件协议运维行为审计，但不影响文件协议会话审计。以便满足客户防范涉密运维行为泄露。
其他要求		中标后七个工作日内，提供样机进行上述功能要求的逐一测试验证，测试中发现虚假应标的行为将取消中标资格并保留追究相关责任的权利。

3、其他补充支持服务

（1）现场支持服务

针对突发事件、新系统上线及其他需要，所有实施现场需按照招标方要求，提供现场技术支持服务。针对重大节日提供 24 小时电话保障，必要时，提供现场保障。

（2）技术培训

提供不少于 3 天的现场培训，培训不限人数。且达到运维人员可根据培训内容处理硬件设备基础配置、排障工作，培训时间由招标方指定。

（3）★特别要求

投标方提供的安全服务，必须在服务器受到攻击的情况下，在第一时间进行阻断和防护，其中服务器包含镇司所有在用服务器，不管是否有没有验收交付；核心服务器为生产运营管理系统服务器和集装箱系统服务器；漏洞分为应用漏洞和非应用漏洞；数据分为关键数据及非关键数据，关键数据包括所有核心服务器数据以及当前在使用的未过期的账户密码、IP 地址、策略、视频数据等；服务器失陷指获得服务器管理员部分或全部权限。

如因应用漏洞问题未及时防护导致服务器失陷，且有任何关键数据泄漏或 2 台及 2 台以上非关键数据泄漏，招标方有权解除合同，并要求投标方支付合同总价 30%的违约金。

如因非应用漏洞问题未及时防护导致任何服务器失陷，并造成严重后果（上级或政府部门对镇司的考核、问责、通报批评等），招标方有权解除合同，并要求投标方支付合同总价 30%的违约金。

因投标方原因未能按本合同约定及时提供维护服务，投标方应向招标方支付违约金，违约金的计算办法为每一次按合同总额的 10%计算。投标方累计 3 次未能按照本合同约定及时提供维护服务的，招标方有权解除合同，并要求投标方赔偿招标方相应的损失。

4、项目验收

在完成安全服务项目实施工作后进行 5 天的试运行期。

投标方应向招标方提供完备的项目验收文档，提交符合合同要求的整个安全加固从设计、安装、调试、测试、验收、试运行全过程以及系统今后运行的维护文档的电子和书面项目可交付物，包括但不限于各类设备配置文档、测试文档、各系统管理文档等验收文档。通过试运行期后由投标方提出验收申请。

验收小组由招标方和投标方共同组成。由投标方提供验收方案，经双方确认后进行系统验收，由投标方提交系统验收报告，双方签署项目验收合格证书。

★5、安全准入要求

5.1 资质合规性：营业执照经营范围应包含项目所须的经营范围，并在有效期内，无被吊销资质的不良记录。

5.2 安全业绩：近 5 年公司所承担业务外包范围内无 1 人死亡及以上安全生产责任事故(含劳务外包人员)；未被列入安全生产严重失信主体名单（可通过“应急管理部”“信用中国”官方网站查询)。

5.3 安全管理机构及安全管理人员配置：依据国家相关法律法规，结合业务类型或企业性质，设置安全生产管理机构或配全配齐专兼职安全管理人员。

5.4 安全教育：从业人员应具备所从事岗位的安全知识和技能，并有教育培训档案。

5.5 从业人员：从业人员文化程度应在初中及以上，身体健康无缺陷，年龄在 18 周岁以上,不允许超过法定退休年龄的人员进场从事重体力劳动作业。从业人员根据岗位需要依法取得行业认可的资格证书。

5.6 劳动合同与工伤保险：业务外包单位必须与所有从业人员签订合法有效的劳动合同，并依法为从业人员缴纳养老保险、工伤保险等。业务外包单位应结合作业风险情况及自身赔付能力，为其从业人员投保第三方人身意外保险。签订合同前需提供相应的劳动合同证明及社保缴纳明细。

5.7 劳动防护用品：为从业人员配备与其作业相匹配的劳动防护用品，且应符合国家标准或者行业标准。

5.8 风险管控清单：对承包项目的主要风险进行辨识，并制定管控措施，建立风险分级管控清单。

5.9 设备保障：设备数量、型号匹配外包业务需求，设备资质及检测情况符合行业标准，设备维护计划可行。

6、网络安全设备维护服务设备清单

设备名称	设备型号	数量	单位
绿盟入侵防御系统 IPS	NIPSNX3-HDCM2401	2	台
奇安信上网行为管理	NBM3245X	2	台
绿盟防火墙	NFNX3-HDCM2620	2	台
奇安信 WAF	W5000-U015P	1	台
绿盟安全管理平台	ESP-HNX3-HDCM1201C	1	台
绿盟综合威胁探针 UTS	UTSNX3-HDCM14-P	1	台
绿盟 EDR	ESS-UESNX1-SN	1	台

深信服视频网防火墙	AF-2000-FH2130B-IG	1	台
绿盟堡垒机	OSMSNX3-1000CM	2	台
绿盟日志审计	LASNX3-HDCM1001	1	台
绿盟数据库审计	DASNX3-HDCM2500	1	台
深信服网闸	GAP-1000-C640	1	台

第三章　投标人须知

前附表

序号	内容、要求
1	项目名称：宁波镇海港埠有限公司 2026 年-2028 年网络安全维护服务项目
★2	投标报价及费用： 1、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。 2、**本次招标控制价 75 万元/年**，超过招标控制价的投标为无效标。
★3	投标保证金：详见招标公告。
4	答疑与澄清：招标人对已发出的招标文件进行必要的澄清和修改时，将在招标公告规定的投标截止时间 3 日前，在规定信息发布网站上通知所有招标文件收受人，并要求收受人进行确认澄清和修改已收悉，澄清和修改的内容作为招标文件的组成部分。招标人根据实际情况，延长投标截止时间的，将在投标截止时间前 2 日内告知所有招标文件收受人，并要求回执确认。
5	投标文件组成：价格标、商务技术标、资审文件。
6	投标截止时间、地址：详见招标公告。
7	开标时间、地址：详见招标公告。
8	评标办法及评分标准：详见第四章。
9	评标结果公示：评标结束后，评标结果于浙江省海港集团、宁波舟山港集团电子招标采购平台（http://hgdzzb.nbport.com.cn/）公示不少于 3 日。
10	投标保证金退还：除招标文件规定不予退还保证金的情形外，最迟在签署合同后 5 日内向投标人退还投标保证金。
11	签订合同时间：中标通知书发出后 30 日内。
★12	履约保证金：无
13	资金来源：自筹。
★14	投标文件有效期：自投标截止日起 60 天。
★15	本项目采用电子招标形式，需对上线交易项目收取交易服务费，交易服务收费标准参照《浙江省物价局关于降低和规范公共资源交易服务收费的通知》（浙价服〔2018〕

<table>
<tr><td></td><td>68 号)的规定，以中标金额为基础，向中标单位收取（具体收费标准见下表）。中标单位须在明确中标后、获取中标通知书前将相应的交易服务费缴入平台指定的集团账户（在“投标管家”工具中查看）。
附表：
招标项目交易服务费收取标准
<table><tr><th>中标价</th><th>收费标准（万元）</th></tr><tr><td>200 万（含）以下</td><td>0.1</td></tr><tr><td>200 万-500 万（含）</td><td>0.25</td></tr><tr><td>500 万-1000 万（含）</td><td>0.75</td></tr><tr><td>1000 万-2000 万（含）</td><td>1.25</td></tr><tr><td>2000 万-5000 万（含）</td><td>1.75</td></tr><tr><td>5000 万-1 亿（含）</td><td>2.5</td></tr><tr><td>1 亿-5 亿（含）</td><td>3.5</td></tr><tr><td>5 亿-10 亿（含）</td><td>5</td></tr><tr><td>10 亿以上</td><td>6</td></tr></table>注:
1.交易服务费由中标单位承担。
2.对于招标服务期在 1 年以上且按每年报价的项目，交易服务费按 1 年的中标金额计取。
3.对于无具体交易(中标)金额的限额以上招标采购项目参照项目计划金额计取,对于无具体交易(中标)金额的限额以下招标采购项目按每个项目 1000 元计取，多家中标人费用平摊。
4.限额以下非招标项目按实际成交价 0.2%收取交易服务费，最高不超过 500 元，5 万元以下项目免收交易服务费。</td></tr>
<tr><td>★16</td><td>本项目招标代理服务费按照“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”的规定收费标准×50%，按照中标金额向中标人收取，不足 2000 元的按 2000 元计取，该费用须在中标人领取中标通知书前一次性付清。</td></tr>
<tr><td>17</td><td>解释：本招标文件的解释权属于招标人。</td></tr>
<tr><td>18</td><td>其他：中标单位中标后须向招标人（招标代理机构）提交纸质投标文件份数 2 份。</td></tr>
</table>

一、总　则

（一）适用范围

本招标文件适用于宁波镇海港埠有限公司2026年-2028年网络安全维护服务项目的招标、投标、评标、定标、验收、合同履约、付款等行为（法律、法规另有规定的，从其规定）。

（二）定义

1. “招标人”系指组织本次招标的单位。

2. “投标人”系指向招标人提交投标文件的单位。

3. “产品”系指供方按招标文件规定，须向招标人提供的一切货物、设备、保险、税金、基础数据、工具、手册及其他有关技术资料和材料。

4. “服务”系指招标文件规定投标人须承担的安装、调试、技术协助、培训、技术指导以及其他类似的义务。

5. “项目”系指投标人按招标文件规定向招标人提供的产品及服务。

6. “书面形式”包括信函、传真、电子邮件等。

7. 带“★”条款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

投标人代表须提供有效身份证件。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。

（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（招标文件有相关规定除外）。

（六）联合体投标

本项目不接受联合体投标。

（七）转包

★本项目不允许转包。

（八）特别说明：

1. 本项目不属于依法必须招标项目，也不属于政府采购项目。

★2. 投标人应仔细阅读招标文件的所有内容，按照招标文件的要求提交投标文件，并对

所提供的全部资料的真实性承担法律责任。

（九）异议和投诉

1. 投标人对招标文件有异议的，应当在投标截止时间 3 日前提出；投标人对评标结果有异议的，应当在评标结果公示期间提出，逾期不予受理。

2. 异议应当在浙江海港电子招标采购平台上提出，投诉应当以书面形式提出。异议书、投诉书均应明确阐述招标文件、招标过程或中标结果中使自己合法权益受到损害的实质性内容，提供相关事实、依据和证据及其来源或线索，便于有关单位调查、答复和处理。

二、招标文件

（一）招标文件的构成。本招标文件由以下部分组成：

1. 招标公告

2. 招标需求

3. 投标人须知

4. 评标办法及评分标准

5. 合同主要条款

6. 投标文件格式

7. 本项目招标文件的澄清、答复、修改、补充的内容

（二）投标人的风险

投标人没有按照招标文件要求提供全部资料，或者投标人没有对招标文件在各方面作出实质性响应是投标人的风险，并可能导致其投标被拒绝。

（三）招标文件的澄清与修改

1. 招标人对已发出的招标文件进行必要的澄清和修改时，将在招标公告规定的投标截止时间 3 日前，在规定信息发布网站上通知所有招标文件收受人，并要求收受人经确认澄清和修改已收悉，澄清和修改的内容作为招标文件的组成部分。招标人根据实际情况，延长投标截止时间的，将在投标截止时间前 2 日内告知所有招标文件收受人，并要求回执确认。

2. 购买招标文件的潜在投标人对招标文件有异议，应在投标截止时间 3 日前书面提出。逾期提出的将不予受理。对招标文件的异议应有法定代表人或其授权代表签章，并盖投标人公章并注明日期。

3. 没有提出异议且又参与了该项目投标的投标人将被视为完全认同招标文件。

三、投标文件的编制

（一）投标文件目录：未提供格式部分由投标人自拟

投标文件分为价格标、商务技术标、资审文件三部分，其内容分别为：

第一部分：价格标

（1）投标函（格式见附件）；

（2）报价表（格式见附件）；

（3）分项报价表（格式见附件）；

（4）投标人针对报价需要说明的其他文件和说明（格式自拟）。

第二部分：商务技术标

（1）评分索引表（格式见附件）；

（2）商务响应表（格式见附件）；

（3）技术响应表（格式见附件）；

（4）综合实力；

（5）同类业绩（格式见附件）；

（6）技术参数响应情况；

（7）认证证书；

（8）人员配备（格式见附件）；

（9）项目总体服务方案；

（10）售后服务；

（11）承诺函（格式见附件）；

（12）商务技术标评审所涉及的其他资料（若有，格式自拟）：

（13）投标人需要特别说明的其他文件（若有，格式自拟）。

第三部分：资审文件

（1）法定代表人资格证明书或法定代表人授权委托书（格式见附件）；

（2）有效的营业执照扫描件；

（3）投标人资格声明函（格式见附件）；

（4）投标人基本情况表（格式见附件）；

（5）投标保证金缴纳凭证；

（6）合格投标人的资格要求业绩证明材料；（若有）

（7）招标文件要求的或投标人认为有必要提供的其他情况说明或资质证书。

注：以上投标资料所要求为扫描件/复印件，均须加盖公章。中标后招标人有权对中标单位相关资料进行原件核实，若有虚假，则取消中标资格，并追究相应责任。

（二）投标文件的语言及计量

★1. 投标文件以及投标人与招标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，招标文件已有明确规定的，使用招标文件规定的计量单位；招标文件没有规定的，应采用中华人民共和国法定计量单位（例如货币单位：人民币元），否则视同未响应。

（三）投标报价

1. 投标报价应按招标文件中相关附表格式填写。

2.投标价格已包含但不限于服务费、维护费、人工费、交通费、培训费、技术服务费、管理费、保险、税金、利润、招标代理服务费、平台交易服务费等所发生的全部费用。如遇国家税率政策调整，则合同价格按照不含税价不变原则进行调整。

3. 投标文件只允许有一个投标总价，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 60 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，招标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而不会导致投标保证金被没收。同意延长有效期的投标人需要相应延长投标保证金的有效期，但不能修改投标文件。

4. 中标人的投标文件自开标之日起至合同履行完毕为止均应保持有效。

（五）投标保证金

★1. 投标人须按规定提交投标保证金。否则，其投标将被拒绝。

2. 保证金形式：电汇；

3. 最迟在签署合同后 5 日内向投标人退还投标保证金。

4. 投标人有下列情形之一的，投标保证金将不予退还：

（1）投标人在投标有效期内撤回投标文件的；

（2）在提交投标文件截止时间后主动对投标文件提出实质性修改的；

（3）投标人在投标过程中弄虚作假，提供虚假材料的；

（4）中标人无正当理由不与招标人签订合同的；

（5）将中标项目转让给他人或者在投标文件中未说明且未经招标人同意，将中标项目分包给他人的；

（6）拒绝履行合同义务的；

（7）其他严重扰乱招投标程序的。

（六）投标文件的签署

1. 投标人应按本招标文件规定的格式和顺序编制投标文件并标注页码，投标文件内容不完整、编排及上传混乱导致投标文件被误读、漏读或者查找不到相关内容的，是投标人的责任。

2. 投标人根据招标文件要求分别提供价格标、商务技术标、资审文件。

★3. 法定代表人授权委托书必须由法定代表人签字或盖法人章、被授权人签章并加盖单位公章。投标文件及投标报价表必须由法定代表人或被授权人签章并加盖单位公章，投标人应写全称。

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

（七）投标文件的递交、修改和撤回

1. 投标文件需在投标文件递交的截止时间前递交。

2. 投标人在投标截止时间之前，可以对已提交的投标文件进行修改或撤回；投标截止时间后，投标人不得撤回、修改投标文件。

（八）投标无效的情形

实质上没有响应招标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销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，但经评标委员会认定属于投标人疏忽、笔误所造成的差错，应当允许其在评标结束之前进行修改或者补正。限期内不补正或经补正后仍不符合招标文件要求的，应认定其投标无效。投标人修改、补正投标文件后，不影响评标委员会对其投标文件所作的评价和评分结果。

出现下列情形之一的，投标文件将被视为无效：

（1）投标人的资格条件不符合招标文件要求的。

（2）投标人未提交投标保证金或保证金金额不足，投标保证金形式不符合招标文件要求的。

（3）投标文件未按招标文件要求签字盖章的。

（4）投标有效期不足的。

（5）在评标过程中，评标委员会发现投标人的报价明显低于其他投标报价，使得其投标报价可能低于其个别成本的，应当要求该投标人作出说明并提供相关证明材料。投标人不能合理说明或者不能提供相关证明材料的，由评标委员会认定该投标人以低于成本报价竞标，其投标作无效标处理。

（6）不同投标人的电子投标文件编制时的计算机硬件信息中网卡 MAC 地址（如有）、硬盘（含移动存储介质）序列号（0ptane_0000、0100_0000_0000_0000 序列号除外）、互联网接入 IP 地址相同。

（7）投标文件实质上没有响应招标文件要求的。

（8）投标文件中附有招标人不能接受的条件的。

四、重新招标

有下列情形之一的，招标人将重新招标：

1. 至招标文件下载截止时间止，下载招标文件的投标人少于 3 个的。

2. 投标截止时间止，投标人少于 3 个的。

3. 评标委员会对所有投标作否决投标处理的，或者评标委员会对一部分投标作否决投标处理后其他有效投标不足三个使得投标明显缺乏竞争，决定否决全部投标的。

五、开标

招标人将在规定的时间和地点进行开标，投标人根据投标文件递交的截止时间前递交。投标人于投标截止时间之后三十分钟内在“浙江海港投标管家”工具端—进入项目—开标—远程开标模块，点击“确认开标结果”按钮进行确认，如超时未确认，视作投标人已对开标结果确认无误。

六、评标

（一）组建评标委员会

本项目评标委员会由评审专家和招标人代表组成。

（二）评标的方式

本项目采用不公开方式评标，评标的依据为招标文件、投标文件及其补充文件（若有）。

（三）评标程序

详见《第四章：评标办法及评分标准》

（四）评标原则和评标办法

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

2. 评标办法。本项目评标办法是**综合评分法**，具体评标内容及评分标准等详见《第四章：评标办法及评分标准》。

（五）评标过程的监控

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。

七、定标

1. 评标结束后，评标结果在浙江省海港集团、宁波舟山港集团电子招标采购平台网站上公示不少于 3 日。

2. 投标人对评标结果无异议的，招标人将确定排名第一的中标候选人为中标人。如有投标人对评标结果提出质疑的，招标人可在质疑处理完毕后确定中标人。

3. 招标人依法确定中标人后，将在浙江省海港集团、宁波舟山港集团电子招标采购平台发出《中标通知书》。

八、合同授予

1. 宁波镇海港埠有限公司与中标人应当在《中标通知书》发出之日起 30 日内签订合同。同时对合同内容进行审查，如发现与招标结果和投标承诺内容不一致的，应予以纠正。

2. 中标人拖延、拒签合同的，将被扣罚投标保证金并取消中标资格。

第四章　评标办法及评分标准

一、总则

宁波镇海港埠有限公司 2026 年-2028 年网络安全维护服务项目采取公开招标形式选择投标人。为保证招标“公开、公平、公正”，根据相关法律、法规，结合本项目的特点，制定本评标办法。

二、评标组织

评标委员会：根据项目的内容特点按照浙江省海港集团、宁波舟山港集团有限公司相关规定组建评标委员会。评标委员会由招标人代表、技术及经济方面专家等有关人员组成。

三、评标程序

1.初步审查

初审分为资格审查和初步评审。

资格审查。依据法律法规和招标文件的规定，对投标文件中的资格证明等进行审查，以确定投标投标人是否具备投标资格。

初步评审。依据招标文件的规定，从投标文件的有效性、完整性、投标保证金和对招标文件的响应程度进行审查，以确定是否对招标文件的实质性要求作出响应。

评标委员会在评审过程中按规定否决不合格投标或界定为无效标后，因有效投标人不足三家的，由评标委员会认定本项目剩余有效投标是否具有竞争性，评标委员会认为有效投标仍然具有竞争性的，对有效投标进行评审；如认为没有竞争性的，招标人将依法重新招标。

2.详细评审

评标委员会对初步评审合格的投标文件，依照本办法对商务技术内容作进一步评审、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评分。

详细评审即以招标文件为依据，对所有实质上响应的投标分别从“商务技术”和“价格”两个方面进行评审并按照评分标准进行打分。

评委评分参照本部分附表：评分标准表。由各评标委员会成员评分，根据投标人的投标文件，进行独立评分。评委评分采用记名方式，取算术平均分（小数点后保留二位小数）。

如有招标文件未规定的情况出现，则由评标委员会集体讨论决定。

2.　错误修正

投标文件如果出现计算或表达上的错误，修正错误的原则如下：

（1）投标文件的大写金额和小写金额不一致的，以大写金额为准；

（2）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；

（3）对不同文字文本投标文件的解释发生异议的，以中文文本为准；

（4）投标文件中出现前后不一致的情况商务部分以商务标为准，技术部分以技术标为准。

按上述修正错误的原则及方法调整或修正投标文件的投标报价，如果投标人接受修正后的报价，则经投标人同意并签字确认后，调整后的投标报价对投标人具有约束作用；如果投标人不接受修正后的报价，则其投标将作为无效投标处理。

4.价格调整的原则

（1）投标人的报价必须包含本次招标范围内所有内容。

（2）投标人报价如有漏项，则须将其他投标人报价中该项价格的最高价加入该投标人的投标总价，调整后的投标总价作为评标价格。但在签订合同时，调整部分的价格不计入合同总价，投标人必须免费提供漏项项目。

（3）如投标人的报价包含了招标范围之外的内容，则投标价格不予调整。但在签订合同时，超出部分设备及相应价格应予以剔除。

（4）如果投标人不接受上述调整原则，则投标文件作无效标处理。

（5）调整后的价格作为投标人的评标价，按照相应的价格评分方式评分。

（6）修正后的最终投标报价若超过招标控制价（如有），评标委员会应否决其投标；修正后的最终投标报价如高于开标一览表的报价，按修正后的最终投标报价作为评标价；修正后的最终投标报价如低于开标一览表的报价，按开标一览表的报价作为评标价，参与价格得分的计算。

（7）签约合同价的确定原则如下：

按照评标办法规定对投标报价进行修正后，若修正后的最终投标报价小于开标一览表的报价的，则签订合同时以修正后的最终投标报价为准；

按照评标办法规定对投标报价进行修正后，若修正后的最终投标报价大于开标一览表的报价的，则签订合同时以开标一览表的报价为准。

5.澄清问题

评标委员会可以书面形式要求投标人对投标文件中含义不明确、对同类问题表述不一致或者有明显文字和计算错误的内容作必要的澄清、说明或者纠正。有关澄清的要求和回复均应以书面形式提交，澄清、说明或者纠正必须有法人或法人授权人签字确认，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，且视为投标文件的组成部分，并汇总纳入评标报告。

6. 中标原则

评标委员会根据各投标人的综合得分高低排定顺序，推荐综合得分最高的投标人为第一中标候选人；综合得分第二的投标人为第二中标候选人。如投标人的综合得分相同，则投标价低者优先；如投标价也相同，则商务技术分高者优先；如商务技术分也相同，则由招标人抽签决定。

7. 评标结果

招标人将中标结果在浙江省海港集团、宁波舟山港集团电子招标采购平台上公示，根据公示和决标结果，向中标人发出中标通知书。

中标人如因自身原因放弃中标或因不可抗力不能履行合同或未按招标文件及投标文件承诺履行的，招标人可选择第二中标候选人为中标人或重新招标。

四、评分标准

本项目评审办法是综合评分法。

满分 100 分，综合评分包括商务技术和价格部分。

商务技术部分、价格部分评分，评标因素及标准详见附表。

评审因素		分值	评分标准说明
价格部分70分	价格分	70	①有效投标人为五家及以下，A=评标基准价=经评审合格的有效投标人评标价的算术平均值*0.98； ②有效投标人为五家以上，A=评标基准价=经评审合格的有效投标人去掉一个最高评标价和一个最低评标价后的算术平均值*0.98。 （此式计算结果保留到整数，小数后第一位四舍五入，以元为单位） B=各有效投标人的评标价，计算价格分方法如下： （1）评标价格为评标基准价的得 70 分； （2）当 B≤A 时，投标人价格得分=70+30×(B-A)/A； （3）当 B＞A 时，投标人价格得分=70-60×(B-A)/A。
商务技术部分30分	综合实力	2	评委对各投标人的综合实力（如企业规模、近三年的主营收入、企业荣誉、银行资信等级、企业资质证书等）进行综合评议。优（1.5-2]，良（0.5-1.5]，一般（0-0.5] **注：投标文件中提供相关的证明材料。**
	同类业绩	3	投标人自 2023 年 1 月 1 日以来（以合同签订日期为准）具有信息网络安全或安全技术服务相关项目服务业绩的,每提供 1 个得 1 分，最高得 3 分。 **注：提供①合同扫描件(包括合同首页、签字盖章页及能反映项目内容等相关合同内容的关键页)、②结算发票扫描件，二者缺一不可并加盖投标人公章。**

	技术参数响应情况	6	根据投标人响应招标文件中技术规格书的符合性进行打分，标注“★”的为实质性条款，负偏离（或未响应）的作废标处理；标注“▲”的为重要条款，每负偏离（或未响应）一项扣 1 分；其余未标注符号的为一般条款，每负偏离（或未响应）一项扣 0.5 分，扣完为止。 **注：技术规格书中要求提供佐证材料的条款，若未提供视为负偏离（或未响应）。**
	认证证书	3	投标人具有①有效的 ITSS 信息技术服务标准符合性证书的得 1 分；②具有有效的信息安全管理体系认证证书的得 1 分；③具有有效的信息技术服务管理体系认证证书的得 1 分。 **注：提供有效的证书复印件并加盖公章。**
	人员配备	6	根据投标人提供的人员证书进行评议（本项总分最高得 6 分）： 1、具有高级网络信息安全工程师证书的每个人得 1 分，本项最高得 2 分； 2、具备注册信息安全专业人员（CISP）证书的每个人得 1 分，本项最高得 2 分； 3、具有信息系统运维管理工程师（高级）证书的得 1 分，本项最高得 2 分； 4、具有重要信息系统保护人员 CIIP-A 证书每个人得 1 分，本项最高得 2 分。 **注：提供人员有效证书复印件及投标人为其缴纳的三个月的社保证明（统一要求 2025 年 10 月-12 月）等，复印件并加盖公章。如同一人拥有多本证书，只按一本计分。**
	项目总体服务方案	6	评委根据投标人提供的项目总体服务方案的完整性、合理性、可行性进行评议，优（4-6]，良（2-4]，一般（0-2]，未提供不得分。
	售后服务	4	根据投标人提供的针对本项目的售后服务承诺（包括响应时间、提升服务要求、应急响应等）进行综合评议，优（3-4]，良（1-3]，一般（0-1]，缺项不得分

注：

1、上述评分表中“(、)”不含本数，“[、]”包含本数。

2、客观分的认定均由评标委员会集体审核确定。

3、有关证书或证明材料复印件/扫描件必须清晰、明了、完整、详细且真实有效。否则由此引起的资格审查不通过，评审内容未得分或少得分及引起的处罚均由投标人负责。

4、投标人在投标文件目录前增加索引页，针对评标办法中的每一个评分项目，注明投标文件内相应的页码，以方便检索。

第五章　合同主要条款

以下合同格式仅供参考，具体以实际签订为准。

宁波镇海港埠有限公司

2026 年度网络安全维护服务合同

甲方（采购方）：宁波镇海港埠有限公司

地址：　宁波市镇海区威远路 111 号

联系人：　　电话：

乙方（供货方）：

地址：

联系人：　　电话：

电子邮件：

鉴于：

甲乙双方本着互惠互利、共同发展的原则，依照《中华人民共和国民法典》的规定，经友好协商，就乙方向甲方提供 宁波镇海港埠有限公司 2026 年度网络安全维护服务项目 事宜签订本合同。

一、安全服务清单

序号	品类	产品名称	描述	数量	备注
1	**安全服务**	资产持续梳理评估	使用绿盟科技的远程漏洞评估产品，检测网络设备、操作系统、数据库和应用服务中存在的安全漏洞及配置并进行资产发现梳理服务，给出相关建议。	8 周	
		渗透测试	通过人工黑盒的测试方式，发现网络和业务系统中存在的安全缺陷，提供复测、渗透测试报告和漏洞修复建议。	4 次/年	
2	**一体化安全运营服务（MDR 服务）**	资产管理服务	安全运营工程师到客户现场，基于绿盟安全运营平台，提供周期性资产核查及资产变更管理服务。	每季度一次	
		脆弱性验证及管理服务	到客户现场提供周期性漏洞扫描或渗透测试，针对中高危漏洞进行准确性验证并给出验证结果，实现漏洞生命周期管理。	每季度一次	

		7*24 远程威胁监测及分析响应服务	绿盟远程运营专家团队，为客户提供 7*24 小时的威胁事件监测及分析服务，并提供处置建议。对常见网络安全事件(挖矿、勒索、蠕虫、入侵等)进行快速响应处置，包括对事件进行预判定性、分析排查、提供遏制方案限制影响扩大、提供清除和修复建议并出具应急响应报告。	一年	
3	**网络及系统安全服务**	持续对资产及业务梳理服务	对生产和办公网终端资产进行持续梳理，对生产和办公网络设备资产进行持续梳理，对生产和办公网安全策略梳理和细化，并提供详细的资产梳理和安全策略梳理记录。	一年	
		安全架构设计与优化服务	帮助企业设计和优化其安全架构，以更有效地防御网络攻击和威胁。	一年	
		服务器系统漏洞加固及业务安全优化服务	服务器系统加固，对生产及办公网服务器系统漏洞的安全加固。 提供生产和办公网业务系统的安全加固建议，以及协助梳理业务及增强安全防护策略。	一年	
		网络安全技术防护策略持续改进服务	帮助企业制定或优化其网络安全策略和操作流程。 实时对安全设备进行日志监控，在设备发现异常行为时，及时通过黑名单、访问控制列表等方式进行拦截处理施。 对安全监测和安全风险检查的结果进行综合分析研判，识别网络安全风险、脆弱性和不合规配置项，从整体网络安全技术防护策略的角度提出准确、有效的改进措施，协助开展策略配置调优，以持续提升安全运行和防护能力。	一年	
		人员技能安全培训服务	为企业员工提供网络安全意识和最佳实践的培训，增强对钓鱼攻击、恶意软件等威胁的识别能力。	一年 2 次	
		合规性评估和咨询	针对行业特定的安全合规要求（如等保 2.0 合规要求），提供合规性评估和改进建议。	一年 2 次	
		重保期间的安全防护服务	针对重要节假日或重要时期的安全保障服务： 增强网络监控：在重保期间加强网络监控，以便及时发现和响应异常活动或攻击。 强化防御措施：提前更新安全系统，如防火墙、入侵检测系统和恶意软件防护，确保所有防御措施都是最新的。 应急准备和响应计划：确保有一个详尽的应急响应计划，并在重保前进行复习和更新。确保关键人员了解他们在应对潜在安全事件中的角色和责任。 备份和数据恢复：在重保期间前确保所有	15 天/年	

			关键安全设备的配置数据都已备份，并验证恢复流程的有效性。 限制访问控制：重保期间可能需要实施更严格的访问控制措施，特别是对于关键系统和数据。 协调沟通：确保安全团队和关键决策者可以在需要时迅速沟通和协调。 审计和合规性检查：进行定期的安全审计，确保符合所有相关法律、法规和行业标准。 灵活调整策略：根据当前的威胁情报和组织的特定需求，灵活调整安全策略和措施。		
		安全事件应急响应处理服务	在发现信息安全威胁后第一时间进行跟进处理，最大限度的降低安全事故带来的危害，减少安全事故带来的影响，将安全损失降到最低； 当入侵或者破坏发生时，对应的处理方法主要的原则是首先保护或恢复计算机、网络服务的正常工作； 然后再对入侵者进行追查，并对整个应急响应过程进行记录。对于紧急事件响应服务主要包括准备、识别事件（判定安全事件类型）、抑制（缩小事件的影响范围）、解决问题、恢复以及后续跟踪。	一年	
		常规网络安全维护服务	安全服务期内，提供以下维护保障：	一年	
			为信息化系统内各个应用系统提供常规维护服务		
			成立技术小组提供 7*24*2 小时技术支持服务		
			提供 7*24 小时服务热线电话，随时响应用户的咨询		
			制定各项业务系统优化策略，保障信息化系统健康稳定运行		
		安全设备运行状态巡视服务	1）每季度 1 次安排安全工程师对生产和办公网涵盖的安全设备进行详细监控检查	一年	
			2）按照计划安排安全工程师对相应系统进行安全巡检并做好记录与总结		
			3）在巡视时如发现设备和系统异常，及时通知相关人员和产品售后服务中心，进行故障处理		
4	**主机安全防护**	EDR 终端安全	绿盟主机安全防护系统许可 20 个 license	1	
5	**堡垒机运维审计**	堡垒机（运维审计）	100 个绿盟堡垒机设备授权(主备堡垒机各 50 个 license)	1	

二、服务费用及支付方式

（一）本合同服务费用总计人民币大写金额：_____（小写：¥_____元），其中

不含税金额：¥_____元，__6__%税额：¥_____元。已包含服务费、维护费、人工费、交通费、培训费、技术服务费、税金等所有费用，乙方不得就服务范围内的服务向甲方收取其他任何费用。

（二）合同签订后 30 天内，甲方凭乙方开具的 50%增值税专用发票支付合同总价的 50%价款。运维服务到期后，甲方确认没有未解决的技术问题后凭乙方开具的 50%增值税专用发票（税率：__6__%）支付合同总价的 50%价款。

（三）一次性支付费用在 10 万元以上的，甲方可以不低于 50%承兑汇票的方式支付服务费用。

（四）付款方式：合同价款由甲方通过银行转账方式支付给乙方：

甲方开票信息如下：

企业名称：_____宁波镇海港埠有限公司_____

纳税人识别号：__91330211MA2J48GC1D_____

地址：__宁波市镇海区威远路 111 号_____

电话：_____

开户银行及账号：工行宁波市镇海区支行 3901160009200161473

乙方的收款账户信息如下：

公司名称：_____

营业执照证号：_____

法人代表：_____

开户行：_____

账号：_____

注册地址：_____

三、服务期限：_____年____月___日至_____年____月____日。

四、技术情报和资料的保密

（一） 如无相反证据，甲方提供给乙方的各类信息都属于保密范围；甲方提供信息时有特别要求的，乙方应遵守。

（二）乙方有权了解其承担的该维护部分包括的所有内容，并负有为甲方保密的义务。

（三）乙方对甲方提供的与项目有关的技术资料、秘密文件不得丢失，不得自行复制，不得向第三方提供，不得用于除履行本合同以外的其他目的，本合同届满后十日内应将前述技术

资料、秘密文件及其载体全部归还甲方。不能归还的，应当予以删除该载体上的保密信息。

五、技术成果的归属

维护中功能调整开发所产生的技术成果归甲方所有。未经甲方许可，包括乙方在内的任何单位或个人不得使用前述技术成果，但乙方为履行本合同使用除外。

六、验收标准和方法

乙方必须保证维护完成的系统符合甲方要求，并正常运行。

甲方在乙方维护完成后 5 个工作日内，对维护工作进行验收，并于 5 个工作日内出具验收报告。

七、违约责任

（一）由甲方原因要求终止合同，甲方应至少提前一个月通知乙方，并根据实际维护月份支付费用（每月按年合同总价平均计算），终止当月按实际维护天数，15 天内（含 15 天）支付半月的费用，超过 15 天按全月费用支付。

（二）由乙方原因要求终止合同，乙方应至少提前一个月通知甲方，并不收取终止维护服务当月的费用。

（三）因乙方原因未能按本合同约定及时提供维护服务，乙方应向甲方支付违约金，违约金的计算办法为每一次按合同总额的 1%计算。乙方累计 3 次未能按照本合同约定及时提供维护服务的，甲方有权解除合同，并要求乙方赔偿甲方相应的损失。

（四）甲方如没有按本合同规定向乙方支付维护费用，每逾期一日，须向乙方支付违约金，违约金的计算办法为每一日按合同应付未付的千分之 一 计算。

（五）任何一方违反本合同约定，除承担本条前两款约定的违约责任外，给对方造成损失的还应承担损失赔偿责任，该损失包括但不限于诉讼费、保全费、担保费、公证费、律师费、交通费、鉴定费、执行费等。

（六）乙方提供的安全服务，必须在甲方服务器受到攻击的情况下，在第一时间进行阻断和防护，其中服务器包含甲方所有在用服务器，不管是否验收交付；核心服务器指生产运营管理系统服务器和集装箱系统服务器；漏洞分为应用漏洞和非应用漏洞；数据分为关键数据及非关键数据，关键数据包括所有核心服务器数据以及当前在使用的未过期的账户密码、IP 地址、策略、视频数据等，非关键数据是指除关键数据之外的数据；服务器失陷指获得服务器管理员部分或全部权限。

如因应用漏洞问题未及时防护导致服务器失陷，且有任何关键数据泄漏或 2 台及 2 台以上

非关键数据泄漏，甲方有权解除合同，并要求乙方支付合同总价 30%的违约金。

如因非应用漏洞问题未及时防护导致任何服务器失陷，并造成严重后果（上级或政府部门对镇司的考核、问责、通报批评等），甲方有权解除合同，并要求乙方支付合同总价 30%的违约金。

八、争议解决和法律适用

（一）对于因本合同产生的或与本合同相关的任何争议，合同当事方应当友好协商解决，也可以通过将该争议提交甲方所在地法院通过诉讼解决，本约定如与法律规定的专门管辖或专属管辖相冲突的，应服从法律的规定。

（二）对于合同中未受争议问题影响的其他条款，在争议解决过程中，双方仍应按合同约定履行。

九、通知与送达

合同一方向对方发出的任何书面通知，只要送至相对方提供的合同首部地址即视为已经送达。采用邮寄方式送达的，交寄日后的第三日即为送达之日。采用 Email 送达的，发出 Email 之日即为送达日。由于合同一方提供的联系信息不准确或变更后未及时通知相对方，造成送达文件被退回的，邮件回执上注明的退回当日视为送达之日。

双方确认，上述地址也视同诉讼送达地址，双方不可撤销地同意，所有诉讼（仲裁）过程中的法律文书通过上述地址送达的，无论受送达人是否签收，或是否有权人签收，均为有效送达。

十、其它

（一）本合同附件为本合同组成部分，与本合同具有同等法律效力。

（二）本合同签订后，经甲乙双方协商一致，可以对本合同有关条款进行变更或者补充，但应以书面形式确认。上述文件一经签署，即具有法律效力并成为本合同的有效组成部分。

（三）项目一切保险、第三方责任险由乙方办理。

（四）乙方须为其施工现场的全部人员办理意外伤害保险并支付保险费，包括其员工及为履行合同聘请的第三方的人员。

（五）本合同壹式伍份，甲方执叁份，乙方执贰份，具有同等法律效力。

（六）本合同及附件自双方盖章之日起生效。

（七）双方签字盖章不在同一日期的，以后签字盖章的日期为本合同的生效日期。

附件：

附件 1：技术规格书

附件 2：港区项目安全管理协议

附件 3：廉洁协议

附件 4：合作伙伴合规承诺书

附件 5：数据安全合作责任承诺书

附件 6：保密协议

甲方（盖章）：　　乙方（盖章）：

代表签字：　　代表签字：

年　　月　　日

附件 1

技术规格书

（签合同时附）

附件 2

港区项目安全管理协议

甲方：宁波镇海港埠有限公司

联系人：　　联系电话：

统一社会信用代码：91330211MA2J48GC1D

乙方：

联系人：　　联系电话：

统一社会信用代码：

为进一步加强镇海港港区安全管理，贯彻“安全第一、预防为主、综合治理”的方针，明确双方安全生产管理职责和权限，切实保障港区生产作业安全，根据《中华人民共和国安全生产法》、《中华人民共和国消防法》等法律法规和港区安全、安保、环保等管理规定，经甲乙双方共同协商，特签订本安全生产管理协议。

一、安全管理目标与边界

1.安全管理目标：杜绝人身触电、高处坠落、机械伤害等事故，确保项目安全实施，实现安全生产“零事故、零伤亡、零污染”目标。

2.安全管理边界：

（1）本协议管理范围涵盖乙方在甲方指定的 办公楼 A 和 B 内，从事所有 网络安全维护服务 等作业活动。

（2）甲方场地与乙方项目实施地点之间的物理隔离点（或电气断开点） 为双方安全管理责任的分界点。分界点一侧由甲方负责安全隔离与监护，另一侧由乙方负责作业安全管控。

二、双方核心安全职责

1.甲方职责：

（1）统一协调与监督：对乙方在港区内的安全生产工作负有统一协调、管理和监督的责任，定期开展安全巡查，及时通报安全隐患。

（2）资质与方案审查：审查乙方的营业执照、项目所必须的资质证书及主要人员资格证书。审查乙方提交的专项施工方案及安全技术措施。

（3）全面安全交底：向乙方书面交底作业现场的具体情况，并履行签字确认手续。

（4）提供安全作业条件：负责办理相关手续，在现场具备安全施工条件后后通知乙方进场。

2.乙方职责：

（1）承担主体责任：乙方是本项目现场安全生产的直接责任主体，对其作业人员、设备及全过程的安全负责，独立承担因自身违规操作引发的安全事情后果。

（2）安全管理机构及安全管理人员配置：公司级安全生产管理机构及专职安全管理人员配备符合国家相关法律法规要求，提供机构设置文件及人员任命书备案；施工现场配备至少1名项目专（兼）职现场安全生产管理人员。

（3）健全安全制度：建立并严格执行本单位的安全生产责任制、安全操作规程、隐患排查治理制度、应急管理制度等。

（4）作业人员要求：项目从业人员年龄在18周岁以上、 法定退休年龄以下；特种作业人员、特种设备作业人员具有合法有效的作业资格证书，持证上岗，并已完成项目专项安全培训和技术交底。

（5）安全教育培训要求：项目从业人员应具备所从事岗位的安全知识和技能，并有教育培训档案。

（6）设备保障要求：主要施工机械、设备、仪器的数量、规格型号符合项目需求，相关机械设备工况良好、证件齐全、检测合格、定期检测维保。

（7）保险要求：为项目从业人员办理工伤保险、人身意外伤害险等有关保险，临聘用工应为其购买相关商业保险，保险期限覆盖整个作业周期。

（8）劳动防护用品要求：为项目从业人员配备的劳动防护用品应符合国家标准或者行业标准。

（9）施工方案要求：

1）编制专项施工方案及安全技术措施，方案需包含工程概况、风险辨识清单、风险分级管控措施、应急预案、施工进度计划等内容，报甲方审核通过后方可实施。

2）对作业过程中可能存在的重大风险（如高压带电作业、高处作业、动火作业等），单独编制专项风险管控方案，明确管控责任人及现场监护要求。

3）服从甲方监管：无条件接受甲方的安全监督、管理和指导，对甲方提出的安全隐患整改要求，在规定期限内完成整改并反馈；不得拒绝、阻碍甲方安全检查，不得擅自更改经审核

的施工方案或作业范围。

三、安全管理要求

1.甲乙双方必须严格遵守国家有关安全生产法律法规和强制性规定的要求，认真执行港区各项安全生产规章制度，不得从事违反或超出国家法律法规、港区规定以及擅自开展有可能危及对方安全的生产经营活动。

2.甲乙双方必须加强自身的安全管理工作，切实履行安全生产主体责任，建立健全各类安全管理制度，加大各类安全设备设施的投入，保障各类生产及辅助设施的完好性。

3.甲乙双方应安排专门安全生产管理联络人员，负责在港区的日常管理工作，并进行沟通协调。

甲方联络人：_____，联系电话_____。

乙方联络人：_____，联系电话_____。

4.甲乙双方对各自人员的安全管理负责，必须按规定对本单位的作业人员定期进行安全教育，接受有关法律、法规、消防安全知识、职业卫生防护和应急救援知识的培训，取得国家相关上岗资格后方可上岗。

5.甲方应按规定为乙方办理相关业务，如进港培训、项目报备、进港施工、作业报备的审批，特殊作业作业票、入港证件的核发，安全管理协议的变更等。

6.甲方应如实告知乙方作业区域内的安全风险及相关预控应急措施，乙方应熟知甲方区域内的各类生产作业风险及各项预控应急措施。

7.乙方应如实向甲方提供签署本协议所需的相关信息及资料并对所提供信息及资料的真实性负责。除经向甲方报备审核过的人员和车辆外，其他乙方人员或车辆未经甲方同意不得进入港区。

8.受乙方委托或因乙方申请进入甲方区域的其他人员视为乙方人员，乙方须按乙方人员标准和要求进行管理。

四、生产作业管理

1.乙方入港作业前应做好各项准备工作，作业期间与甲方保持联络，并安排人员对作业状况进行现场监管。

2.乙方有义务向甲方提交作业的安全防范措施、可以证明进入码头人员身份的有效证件、主管部门对当次作业的批复等文件，上述文件未提供，甲方可对作业不予同意或安排。

3.乙方必须从甲方指定地点进入港区。进入港区后，车辆安全文明行驶，规范停放；相关

车辆和人员不得进入与乙方作业无关的区域；作业完毕的车辆和人员，及时离开港区，不得逗留。

4.乙方在甲方区域内作业期间，不得占用消防设施、消防通道、公共道路，作业结束后工完场清。乙方在甲方区域产生的所有垃圾及污染有害物质等与乙方有关的废物由乙方负责带离甲方区域并进行无害化处理，并向甲方提供处理此类物质依据(危险废物转移联单)的复印件。

5.甲方应根据乙方的作业申请，安排管理人员对乙方作业人员的安全行为进行监督管理，有权对乙方在甲方区域内使用的设施、安全防护用品、员工行为等进行检查和抽验，对不符合安全要求的有权要求拆除、更换、整改，并将查实情况及处理意见及时反馈给乙方，但此项检查和评估不得视为甲方对乙方场所、人员及设备安全性的确认和保证。

6.甲方对乙方人员的违章行为，乙方设备设施的安全隐患，有建议权、制止权、考核权、停止合作权。

五、作业安全规范

1.乙方必须严格执行以下强制性安全规范：

工作票制度：变电所内作业必须办理相应工作票，严禁无票作业；工作票需经甲方审核签发后方可生效。

技术措施：施工作业前必须严格落实“停电、验电、装设接地线、悬挂标识牌和装设遮栏”四项技术措施。接地线的装设位置和数量必须符合安全规程，并记录在案。

个人防护：所有人员必须正确穿戴合格的个人防护用品（绝缘鞋、绝缘手套、长袖工作服、安全帽等）。高处作业必须系挂安全带。

现场隔离：在作业区域设置安全警戒线和警示标志，严禁擅自扩大工作范围或移动安全遮栏。

工器具管理：所有自备的安全工器具、仪器仪表必须经检测合格且在有效期内，严禁使用不合格的工器具。

2.乙方未经甲方同意不得擅自动用甲方设备设施。

3.乙方须确保进入甲方区域的乙方设备设施性能完好，资质符合。

4.甲乙双方对可能影响对方的作业应事先进行通报。施工检修中涉及的动火作业、受限空间作业、盲板抽堵作业、高处作业、吊装作业、临时用电作业、动土作业、断路作业等特殊作业；针对特殊作业，乙方需提交专项施工方案给甲方进行审核，并开具特殊作业作业票，甲乙双方必须严格按照港区相关规定执行。

六、隐患整改权责

1.甲方权利：甲方安全管理人员有权随时对作业现场进行检查。发现“三违”（违章指挥、违章作业、违反劳动纪律）行为或事故隐患时，有权立即制止，并视情节发出《安全隐患整改通知书》或责令停工整顿。

2.乙方责任：乙方是隐患整改的第一责任人。应制定安全检查计划定期进行自检自纠，配合开展各类安全检查，对发现的问题按期完成整改。对于甲方提出的隐患，必须立即组织整改，做到“定人、定时间、定措施”，并将整改结果书面回复甲方，形成闭环管理。

3.严重违章处理：对于“无票作业”、“未经验电即作业”、“擅自穿越安全遮栏”等严重危及生命的违章行为，甲方有权对责任单位和责任人进行经济处罚，并责令其退场。

七、应急处置分工

1.乙方应建立自己的应急机制，在甲方区域内发生与乙方有关的安全事件/事故时，甲乙双方应积极参与配合抢险救援工作。

2.遇有紧急情况，乙方在甲方场地内的所有人员、设备设施应服从甲方统一指挥管理或根据现场设置的应急疏散标志快速撤离。

3.应急分工：

乙方：作为现场第一响应人，负责事故初期的紧急处置，包括但不限于：迅速切断电源（在安全前提下）、对触电者进行心肺复苏、使用灭火器扑救初起火灾、疏散现场人员，并立即向甲方现场负责人报告。

甲方：负责启动公司级应急预案，协调内外部应急资源（如医疗、消防），指挥现场救援，并按规定向上级单位和政府主管部门报告。

4.预案与演练：乙方的现场应急处置方案必须报甲方备案，并定期参与甲方组织的联合应急演练。

5.事故报告：乙方发生任何安全事故或未遂事件，必须在 5 分钟内向甲方报告，不得迟报、漏报、瞒报。

八、安全监管与考核

1.乙方应向甲方缴纳本协议履约保证金人民币___/____元，当乙方结束与甲方业务时可向甲方书面申请退还履约保证金，甲方在扣除因违约扣除部分后，无息退还剩余履约保证金。

2.监管方式：甲方采用日常巡查、专项检查、远程监控等方式对乙方进行安全监管。

3.考核评价机制：

（1）甲方依据公司规定，建立健全业务外包单位安全生产管理考评办法，细化量化考核细则。甲方将每季度召开考评会议，按照《相关方考评表》对乙方进行综合考评。

（2）考核内容涵盖但不限于：作业人员安全行为、事故与隐患管理、安全教育培训、安全交底、风险辨识等。

（3）考评结果实行奖优罚劣。对安全管理到位、成绩显著的乙方，甲方可给予通报表扬、经验分享、优先合作等正向激励。对考核不合格或存在问题的乙方，甲方将依据本协议及主合同约定进行处理。

4.乙方人员清退情形：

乙方作业人员及管理人员在合同期内出现以下情形之一的，甲方有权要求乙方立即将该人员清退出场，且乙方应在接到甲方通知后 24 小时内执行。该人员视同被甲方清退：

（1）因违章指挥、违规作业或违反劳动纪律等行为，导致发生重伤及以上生产安全责任事故的。

（2）违章冒险作业情节严重，存在较大亡人风险，且现场拒不停止作业、不服管理的。

（3）吸毒或携带违禁物品（如枪支、弹药、管制刀具、易燃易爆品等）进入作业现场，经查实的。

（4）持用虚假特种作业操作证、身份证、资质证书等入职，或冒名顶替、伪造履历，或隐瞒重大职业健康禁忌，经查实的。

（5）接连发生习惯性违章行为，经甲方或乙方多次教育、警告仍不改正的。

（6）因故意或重大过失行为，导致甲方或甲方公司遭受 50 万元及以上直接经济损失，或造成重大负面舆情影响的。

（7）专（兼）职安全生产管理人员未按法规及合同要求履行安全管理职责（如未开展规定频次的现场检查并记录、未开展安全教育并记录），经甲方指出后仍不配合整改或整改不到位的。

（8）管理人员无正当理由，拒绝或消极应对甲方提出的合理整改要求，拒不整改的。

（9）发生其他法律、法规、甲方规章制度明确禁止的行为。

5.清退程序：

（1）调查核实：甲方发现乙方存在上述第 4 点乙方人员清退情形的，将在 10 个工作日内组织初步调查，收集证据（事故报告、违章记录、考核结果、影像资料等）。甲方内部将对清退的必要性及潜在影响进行评估。若决定启动清退，将形成清退方案。

（2）清退告知：甲方向乙方发出书面《清退告知书》，载明清退理由、事实依据、拟作出的

清退决定及依据的合同条款。乙方有权在收到告知书后 5 个工作日内向甲方提交书面陈述或申辩材料，甲方需在 10 个工作日内组织回复。

（3）审核决定：甲方将充分考虑乙方的陈述申辩意见，结合调查结果，在合理期限内作出最终决定。如决定清退，则向乙方出具《清退决定书》。

（4）落实执行：甲方通知乙方终止外包合同，办理业务交接手续（明确剩余作业、设备、人员的交接方案），及时完成清退工作。

（5）档案更新：清退完成后，甲方将清退决定书报公司业务外包用工管理中心备案，并将业务外包单位清退原因、处理结果录入公司“业务外包信息化管理系统”，公司业务外包用工管理中心将其纳入业务外包单位黑名单，并在平台公示。

6.清退后黑名单管理：

（1）个人黑名单：依据上述第 4 点乙方人员清退情形被清退的个人，自清退决定生效之日起 5 年内，不得以任何形式参与甲方任何业务外包工作。

（2）单位黑名单：依据上述第 4 点乙方人员清退情形被清退的乙方单位，自清退决定生效之日起 2 年内，不得参与甲方任何外包业务投标或合作。同时，乙方的法定代表人（或主要负责人）、实际控制人、对本项目安全直接负责的安全负责人、安全管理人员，以及对导致清退的生产安全责任事故负有直接责任的人员，一并纳入上述黑名单，适用相同的禁入期限。

（3）黑名单信息将在甲方公司指定平台进行公示。禁入期满后，乙方如需重新申请准入，须经甲方公司业务管理部门评估批准。

7.乙方所有进入甲方区域的人员必须服从甲方管理人员的管理，对于违反甲方管理规定的乙方人员，甲方可根据港区管理规定对乙方的违章违纪和不安全行为实施扣除协议履约保证金(具体金额按（镇港安环[2022]108 号）文件《安全生产违章考核处罚细则》)、停工（停运）整改和禁止乙方进港经营（终止本协议及相关业务合同）等措施。乙方对其从业人员的违法和违章违纪行为及因此所造成的后果和所产生的影响负责。

8.甲乙双方发生各类事故时，应及时向对方通报，并按规定程序向有关部门报告，接受有关部门的事故处理，并根据事故责任划分（以交警、安全管理部门或当地政府事故处理责任部门出具的事故责任判定书为准），由各自承担相应事故责任及经济赔偿。

9.发生事故后，乙方弄虚作假、隐瞒不报、迟报或谎报的，一经查出，甲方有权扣除乙方缴纳的全部履约保证金；情节严重的，甲方有权解除合同合作关系并由乙方承担相应后果。

10.本协议具有真实性和有效性，甲乙双方应在协议有效期内严格履行各自管理责任，自

觉遵守本协议各项条款。甲乙双方因违反本协议和有关规定的应承担相应的法律责任。造成对方或第三方经济损失的，责任方应予赔偿。

11.本协议是主合同不可分割的一部分，与主合同具有同等法律效力。主合同中有关安全、考核、违约责任及终止的条款与本协议不一致的，以本协议约定为准。

12.本协议所述“重伤”、“责任事故”、“经常性严重违章”等术语的定义，参照国家有关法律法规、行业标准及甲方公司相关规章制度执行。

13.因本协议的履行或解释发生任何争议，双方应友好协商解决；协商不成的，按主合同约定的争议解决方式处理。

14.本协议自双方盖章后生效，有效期与主合同有效期保持一致，随主合同的终止、解除或履行完毕而自动失效。

九、其他

1.本协议未尽事宜，由双方协商一致后签订补充协议，补充协议与本协议具有同等法律效力；协商不成的，可向甲方所在地人民法院提起诉讼。

2.本协议一式贰份，甲方执壹份，乙方执壹份，经双方盖公章或合同章后立即生效，本协议有效期与主合同有效期一致。

甲方（盖章）：　　乙方（盖章）：

年　月　日　　年　月　日

附件 3

廉洁协议

甲方：宁波镇海港埠有限公司

联系人：　　联系电话：

联系地址：

电子邮件：

乙方：

联系人：　　联系电话：

联系地址：

电子邮件：

为进一步完善监督制约机制，防止发生各种谋取不正当利益的违法违纪行为，促使双方工作人员在履行合同过程当中廉洁自律、诚实守信，保护双方合法权益，根据国家有关法律法规及廉政建设的规定，在签订主合同的基础上，甲乙双方签订本廉洁协议。

1.甲乙双方共同权利义务

1.1 协议双方必须恪守“诚信、公正、科学”的原则，按照主合同要求，把保质保量和及时完成项目作为各自最终的权利和义务，严禁损害企业和各方的合法利益。

1.2 协议双方必须经常教育各自职员严格遵守国家的法律、法规和政策，遵守党的纪律和各项廉洁规定，遵守社会公德和职业道德，防止一切违纪违法行为的发生，使主合同权利义务履行过程同时成为党风廉洁建设的过程。

1.3 双方建立健全的自我制约制度，开展廉洁教育，监督并认真查处各自职员的违法违纪行为。

1.4 发现对方在经济业务活动中有违反本协议约定的不廉洁行为，有及时提醒和督促对方纠正的权利和义务；情节严重的，均有权向有关部门检举、揭发和控告。

2.甲方廉洁义务

甲方，且甲方应教育、督促其职员遵守如下约定：

2.1 不得以任何形式向乙方索请、索礼、索贿或报销应由甲方支付的各类费用；

2.2 不得收受乙方赠送的礼品、礼金、礼券、礼卡和有价证券、股权、其他金融产品等财物；

2.3 不得以明显低于市场的价格向乙方购买商品和物资；

2.4 不得参加由乙方提供经费的旅游或任何类似活动；

2.5 不得接受乙方承担费用的可能影响公正执行公务的宴请和娱乐活动；

2.6 不得向乙方介绍亲属或亲友从事与甲方工作有关的经济活动或推销物资和商品；

2.7 不得接受乙方提供的公车、住房装修等服务。

2.8 不得接受乙方其他任何形式的与业务无关的金钱利益。

3.乙方廉洁义务

乙方，且乙方应教育、督促其职员遵守如下约定：

3.1 不得向甲方工作人员送礼、行贿或提供应由甲方自己支付的各类费用报销；

3.2 不得违规宴请甲方工作人员或提供其他消费娱乐活动；

3.3 不得以明显低于市场的价格向甲方工作人员提供物资和商品；

3.4 不得安排甲方工作人员的子女或其他亲属到本单位工作，双方有业务之前已经安排的，则不得因双方业务关系而特别提升职务或提高待遇；

3.5 不得提供资金邀请甲方工作人员和/或其子女、亲属旅游；

3.6 不得为甲方工作人员的子女或亲属购买或提供商品；

3.7 不得向甲方工作人员提供公车、住房装修等服务。

3.8 不得向甲方提供任何形式的与正当业务往来无关的金钱利益。

4.违约责任

4.1 乙方违反本协议约定，由此给甲方造成损失的，应依法予以赔偿。

4.2 甲方违反本协议约定，由此造成乙方损失的，甲方应承担赔偿责任。

4.3 各方职员违反本协议的，由各方向对方承担违约责任。

5.附则

5.1 本协议作为合同的附件，与主合同具有同等法律效力。经双方盖章后立即生效，有效期与主合同一致，在合同有效期内不可撤销。

5.2 本协议不影响甲乙双方按主合同条款承担相关责任。

甲方：（盖章）　　乙方：（盖章）

附件 4

合作伙伴合规承诺书

为满足宁波镇海港埠有限公司（以下简称“镇司”）及其下属单位合规管理要求，规范本公司市场交易行为，促进公平、公正交易，本公司特作出以下承诺：

1.本公司理解镇司合规管理需求，在合作范围内遵守镇司对第三方的合规管理要求。

2.本公司具有合同订立的主体资格，具有良好的资信和履约能力，能够有效履行合同义务。

3.本公司严格遵守国家法律法规，恪守商业道德和职业道德规范，不从事并抵制任何不廉洁行为，严格履行以下合规义务：

（一）本公司员工严格遵守《中华人民共和国反不正当竞争法》等有关商业贿赂行为的禁止性规定，坚决抵制商业贿赂。

（二）本公司员工不得给予镇司及相关单位或个人的任何不正当馈赠。

（三）本公司员工不得接受镇司及相关单位或个人的任何不正当馈赠。

（四）本公司员工不得参加镇司及有关单位安排的可能影响公正执行公务的宴请、旅游、考察等活动。

（五）本公司员工不得从事其他可能影响廉洁商业的行为。

4.本公司坚持诚信商业行为，依法依约保守镇司的商业秘密。

5.本公司严守缔约精神，全面履行合同义务，不擅自变更、中止以及不履行合同，发生履约突发事件时将当及时通知镇司。

6.本公司同意在合同目的范围内配合镇司的合规检查，不得隐瞒可能造成镇司利益受损的信息。

7.本公司承诺对本承诺书执行情况进行监督检查，本公司及员工未遵守承诺事项，本公司承诺自愿赔偿由此给镇司造成的损失，或按相关合同约定承担违约责任，且镇司有权终止相关合同。

承诺单位（盖章）：

附件 5

数据安全合作责任承诺书

鉴于贵、我双方就该造项目进行合作,现我司就合作中的数据安全责任事宜做出郑重承诺,并严格遵守以下规定:

1、我司承诺恪守良好的职业道德，自觉遵守《中国人民共和国网络安全法》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》等国家有关信息安全的方针政策、法律法规、行政规定；严格执行宁波镇海港埠有限公司各项信息安全规章制度。

2、我司承诺严格遵守宁波镇海港埠有限公司关于信息管理、信息安全等方面的规定，除为履行我司在前述项目中的义务外，不以任何方式利用工作过程中知悉获得的设备口令、帐户信息、任何加解密程序和软件、加解密数据文件、测试工具和软件以及业务合作中知悉获得的任何客户信息等。

3、在涉及宁波镇海港埠有限公司用户数据的各系统、平台以及业务合作的相关工作时，我司承诺采取有效措施保护宁波镇海港埠有限公司的企业数据和用户信息，切实保障国家、社会、企业及客户利益。

4、未经宁波镇海港埠有限公司和所涉及的用户事先书面同意，我司承诺不使用（除非为履行前述项目下我司义务）、泄漏、传播、公布、发布、传授、转让或以其他任何方式让第三方知悉宁波镇海港埠有限公司的保密信息、企业数据、用户信息，以及虽属他人但宁波镇海港埠有限公司负有保密义务的技术秘密、商业秘密、个人隐私等。

5、我司承诺在开展前述项目业务合作的过程中始终同时具备以下几个履约条件：

（1）具备履行项目所需的网络信息服务安全保障措施，在存储数据信息的系统受到网络攻击时能够采取必要措施、手段进行有效防护；

（2）有符合项目履行需要的专业管理人员和信息技术人员；

（3）能够对数据安全类的合作实施有效保护和管理。

6、本承诺书所涉及的各类数据信息仅限我司用于该项目/业务的合作，除此之外任何情形下我司一旦使用基于本项目所知悉获得的数据和用户信息均被视为我司违反本承诺书。

7、我司确认我司职员在工作期内和离职脱秘期内所有与贵司数据信息相关的行为均为职务行为。若我司职员违反承诺，未按照本承诺书规定使用数据信息，或未遵守数据安全管理规

定造成信息泄露，包括但不限于向除贵、我双方外的第三方披露数据及用户信息，或使用基于本项目所获得的数据和用户信息向第三方作出任何建议或进行任何研究开发，均视为我司违反本承诺。

8、如违反本承诺，我司将承担因此给贵司造成的一切损失，包括直接损失和间接损失。

承诺人（盖章）：

附件 6

保密协议

甲方：宁波镇海港埠有限公司

联系人：

联系地址：浙江省宁波市镇海区威远路 111 号

联系电话：

统一社会信用代码：91330211MA2J48GC1D

乙方：

联系人：

联系地址：

联系电话：

统一社会信用代码：

甲乙双方之间拟开展主合同项目合作，合同一方（以下称“披露方”）将向另一方（以下称“接收方”）披露相关信息或提供相关资料（以下简称“保密信息”），为了加强保密信息保护，防止因保密信息泄露给披露方造成不利影响和/或经济损失，经双方协商一致，订立本协议。

1.保密主体

1.1 接收方是保密主体，对从披露方处所获取的保密信息承担保密责任，本协议中的接收方和披露方为（3）：

（1）甲方为披露方，乙方为接收方；

（2）乙方为披露方，甲方为接收方；

（3）甲乙双方互为披露方和接收方。

1.2 本协议中接收方包括接收方、接收方的关联方、接收方和其关联方的董事、监事、管理人员和员工、接收方和其关联方聘请的中介服务机构。

2.保密信息

2.1 保密信息是指无论本协议签署之前或之后，披露方和/或其代表以口头方式和/或书面方式披露给接收方的与本项目相关的任何非公开信息，包括商业信息、技术信息以及其他具有保密性质的信息，无论这些信息是记载在纸质形式、电子数据形式，或者其他任何形式的载体上，无论是否由披露方明确标注“保密”字样，无论是由披露方、披露方的关联方、披露方和其关联方的董事、监事、管理人员和员工、披露方和其关联方聘请的中介服务机构、对披露方负有保密义务的任何第三方直接或间接向接收方披露的信息，均属保密信息。但下列信息不属于保密信息：

2.1.1 披露前已成为公知信息，并可以在公众领域能自由查询到的信息；

2.1.2 披露后由披露方自行向公众领域公开的信息；

2.1.3 披露方明确表示无保密要求的信息；

2.2 商业信息包括但不限于：会议记录、会议纪要、备忘录；经营战略、经营方针、经营规划、经营决策；采购信息、销售信息、价格方案、客户信息；业务流程；财务信息；规章制度、管理方法；企业发展规划、可行性分析资料；合同、协议、意向书及其他任何不被公众领域所知的信息；

2.3 技术信息包括但不限于：专利实施、技术方案；制造方法、配方、工艺流程；技术指标；工程设计、电路设计、计算机软件、数据库、源程序、技术报告、研发记录；检测报告；实验数据、试验结果；图纸、样品、模型、模具；操作手册及其他任何不被公众领域所知的信息；

2.4 根据法律或者相关协议约定披露方负有保密义务的第三方信息。

3.保密要求

3.1 接收方对于来自披露方或其他途径获悉的保密信息负有完全和严格的保密义务。除非为了执行本项目之目的，并经披露方事先书面同意，接收方不得为自己或他人的利益使用、允许使用、转让、复制、传授、泄漏保密信息；接收方不得对保密信息进行分析并从该等分析中获利；

3.2 接收方应以一切的合理手段且不低于接收方自身对类似保密信息所采取的措施来保护保密信息，并应严格限定接收方内部知悉保密信息的人员范围，接收方应要求其获悉秘密信息的所有人员采取必要的措施对收到的秘密信息进行保密，避免任何第三方及接收方的无关人员以任何方式获得此保密信息；

3.3 接收方保证其在合作中有必要知晓保密信息的符合第 1.2 条情形的所有人员，受到与

本协议同等严格保密责任的约束，接收方应对前述人员违反保密要求的行为承担全部责任；

3.4 接收方在收到任何第三方以任何方式发出的对于涉及本协议的保密信息的询问、求证、访问时，应以该保密信息不知情者的身份用“不知道、不清楚、不了解”等方式做出回复。任何类似于“是”或“不是”等明确的肯定或否定的答复均被视为对保密义务的违反；

3.5 披露方的保密信息的部分或个别要素虽被披露成为公知信息，但该信息的其它部分或整体尚未成为公知信息的，接收方仍应按本协议约定对未公开部分的信息履行保密义务；

3.6 因中华人民共和国监管部门要求提供，或者司法机关依职权要求接收方提供相关保密信息的，接收方应当自接到通知之日当天以书面形式告知披露方，并将监管部门或司法机关要求提供保密信息的法律文件原件（或加盖接收方印章的复印件）转给披露方，经披露方同意后方可提供；

3.7 无论因为何种原因导致双方合作目的未予实现，接收方应当在披露方通知之日起 3 日内返还并销毁其所获取的所有保密信息及保密信息载体，接收方不得以任何理由和方式保留。

4.保密期限

4.1 保密期限为 5 年，自本协议生效之日起算，但如果某项保密信息在保密期限内被披露方公开披露或成为公开信息的，则该项保密信息的保密期限可以立即终止，但其他保密信息的保密期限继续有效；

4.2 本协议生效前，披露方已经披露给接收方的保密信息的保密期限自接收方收到该等保密信息之日起算，终止日期按 4.1 条约定执行。

5.违约责任

5.1 在披露方提供的保密信息送达接收方之后，该保密信息因被盗、被抢、丢失等意外原因被泄露，由接收方承担责任，本协议所称送达，是指：（1）面对面交接保密信息的，交接当时为送达；（2）以信件形式寄送的，由接收方任何部门或人员签收即为送达；（3）以电子邮件、微信或其他即时通讯方式发送的，发送成功当时即为送达；（4）以传真方式送达的，披露方传真发送成功为送达；

5.2 因接收方提供错误的电话号码、传真号码、电子邮箱、邮寄地址、微信号、信息接收人等联系方式导致保密信息被泄露，由接收方承担责任；

5.3 接收方违反保密义务的，披露方可以解除主合同（如有），且要求接收方赔偿披露方因此所遭受的全部直接和间接经济损失，经济损失无法计算的，则应向披露方赔偿 壹拾万 元；

5.4 前款所称披露方的损失，包括但不限于直接经济损失、间接经济损失、商誉损失、调查

取证费、公证费、诉讼仲裁费、律师费、其它费用；

5.5 除要求接收方承担经济赔偿责任外，披露方还可依法将接收方违反保密义务的行为向国家有关机关举报。

6.争议的解决

6.1 对于因本协议产生的或与本协议相关的任何争议，协议当事方应当友好协商解决，或者在第三方主持下调解解决，也可以通过下列第（1）种方式解决：

（1）将该争议提交（甲方所在地）**（注：可填写：原告所在地、被告所在地、甲方所在地、乙方所在地、不动产所在地、协议主要义务履行地、协议签订地，或其他标准）**法院通过诉讼解决，本约定如与法律规定的专门管辖或专属管辖相冲突的，应服从法律的规定。

（2）将争议提交（/）仲裁委员会**（注：具体填写规范的仲裁机构名称）**，按照申请仲裁时该会有效的仲裁规则在（/）**（注：填写具体的仲裁地点，仲裁地点可以与仲裁机构所在地不同）**通过仲裁方式解决。仲裁庭的组成应有 3 名仲裁员，仲裁裁决是终局的，对双方均有约束力。

6.2 对于协议中未受争议问题影响的其他条款，在争议解决过程中，双方仍应按协议约定履行。

7.通知与送达

协议一方向对方发出的任何书面通知，只要送至相对方提供的协议首部地址即视为已经送达。采用邮寄方式送达的，交寄日后的第三日即为送达之日。采用 Email 送达的，发出 Email 之日即为送达日。由于协议一方提供的联系信息不准确或变更后未及时通知相对方，造成送达文件被退回的，邮件回执上注明的退回当日视为送达之日。

双方确认，上述地址也视同诉讼送达地址，双方不可撤销地同意，所有诉讼（仲裁）过程中的法律文书通过上述地址送达的，无论受送达人是否签收，或是否有权人签收，均为有效送达。

8.其他

8.1 本协议自双方盖印章起生效，自双方协议义务履行完毕时终止。

甲方（盖章）：　　乙方（盖章）：

日期：　　日期：

第六章 投标文件格式

投标文件目录：未提供格式部分由投标人自拟

投标文件分为价格标、商务技术标、资审文件三部分，其内容分别为：

第一部分：价格标

（1）投标函（格式见附件）；

（2）报价表（格式见附件）；

（3）分项报价表（格式见附件）；

（4）投标人针对报价需要说明的其他文件和说明（格式自拟）。

第二部分：商务技术标

（1）评分索引表（格式见附件）；

（2）商务响应表（格式见附件）；

（3）技术响应表（格式见附件）；

（4）综合实力；

（5）同类业绩（格式见附件）；

（6）技术参数响应情况；

（7）认证证书；

（8）人员配备（格式见附件）；

（9）项目总体服务方案；

（10）售后服务；

（11）承诺函（格式见附件）；

（12）商务技术标评审所涉及的其他资料（若有，格式自拟）：

（13）投标人需要特别说明的其他文件（若有，格式自拟）。

第三部分：资审文件

（1）法定代表人资格证明书或法定代表人授权委托书（格式见附件）；

（2）有效的营业执照扫描件；

（3）投标人资格声明函（格式见附件）；

（4）投标人基本情况表（格式见附件）；

（5）投标保证金缴纳凭证；

（6）合格投标人的资格要求业绩证明材料；（若有）

（7）招标文件要求的或投标人认为有必要提供的其他情况说明或资质证书。

注：以上投标资料所要求为扫描件/复印件，均须加盖公章。中标后招标人有权对中标单位相关资料进行原件核实，若有虚假，则取消中标资格，并追究相应责任。

第一部分：价格标

1. 投标函

投标函

致_____（招标人）：

根据贵方_____（项目名称）_____的招标公告（项目编号：_____），我方递交投标文件价格标__1__份、商务技术标__1__份、资审文件__1__份。

据此函，签字代表宣布同意如下：

1.提供投标须知规定的全部投标文件。

2.总投标价为人民币（大写）：_____元/年；

（小写）：_____元/年。

3.投标人已详细审查全部“招标文件”，包括修改文件（如有）以及全部参考资料和有关附件，已经了解我方对于招标文件、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。

4.投标人在投标之前已经与贵方进行了充分的沟通，完全理解并接受招标文件的各项规定和要求，对招标文件的合理性、合法性不再有异议。

5.本投标有效期自开标日起 60 日历天。

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

7.投标人同意按照贵方要求提供与投标有关的一切数据或资料。

8.投标人同意按招标文件规定交纳投标保证金、中标服务费，遵守所有有关招标的各项规定。

9. 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：_____

投标人代表姓名：_____ 职务：_____

投标人名称（公章）：_____

开户银行：_____ 银行帐号：_____

法人代表或授权代表签章: _____

日期：_____年___月___日

2. 报价表

报价表

序号	内　　容	投标总价	备注
1	宁波镇海港埠有限公司2026年-2028年网络安全维护服务	大写：_____元/年 小写：¥_____元/年 税率：__6__%	
服务期限：三年。合同一年一签，根据上一轮合同的履约情况，双方协商一致后可续签下一年度的合同。			
服务地点：宁波镇海港埠有限公司（招标人指定地点）。			

注：投标价格已包含但不限于服务费、维护费、人工费、交通费、培训费、技术服务费、管理费、保险、税金、利润、招标代理服务费、平台交易服务费等所发生的全部费用。如遇国家税率政策调整，则合同价格按照不含税价不变原则进行调整。

法定代表人或授权代表（签章）：

投标人名称（盖章）：

日期：　年　月　日

3. 分项报价表

分项报价表

单位：人民币元

序号	内容	单位	数量	单价	总价	备注
1						
2						
3						
4						
5						
……						
合计						

注：分项报价表中的“合计”应与投标函中的“总投标价”和开标一览表中的“投标总价”保持一致。

法定代表人或授权代表（签章）：

投标人名称（盖章）：

日期：　年　月　日

4、投标人针对报价需要说明的其他文件和说明（格式自拟）。

第二部分：商务技术标

1. 评分索引表

评分索引表

序号	评分内容	评分标准	证明材料所在页码
1			
2			
3			
4			
5			
6			
7			
8			

2. 商务响应表

商务响应表

招标编号：　　项目名称：

条款号	招标文件要求	投标人的承诺和说明	偏离情况
……			

注：主要针对招标文件第二章　招标需求的“商务要求”内容逐条响应，并在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”，如未注明，招标人则视投标人完全接受和满足招标文件规定的要求。

法定代表人或授权代表（签章）：

投标人名称（盖章）：

日期：　年　月　日

3. 技术响应表

技术响应表

招标编号：　　项目名称：

条款号	名称	招标文件技术需求	投标人的承诺和说明	偏离情况

注：投标人应对照招标文件第二章　招标需求的“技术规格书”内容进行响应，并在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”，如未注明，招标人则视投标人完全接受和满足招标文件规定的要求。

后附：原厂针对本项目的服务承诺函，内容包括：①绿盟主机安全防护系统的许可 20 个 license，并提供一年原厂服务；②绿盟堡垒机 100 个 license(主备堡垒机各 50 个 license)，并提供一年原厂服务。（格式自拟）

法定代表人或授权代表（签章）：

投标人名称（盖章）：

日期：　年　月　日

承诺函

（格式自拟）

内容包括：①绿盟主机安全防护系统的许可 20 个 license，并提供一年原厂服务；②绿盟堡垒机 100 个 license(主备堡垒机各 50 个 license)，并提供一年原厂服务。

4. 综合实力

5.同类业绩

同类项目业绩表

序号	项目名称 （主要实施内容）	采购方	合同签订时间	合同价	联系人、 联系方式

注：提供①合同扫描件(包括合同首页、签字盖章页及能反映项目内容等相关合同内容的关键页)、②结算发票扫描件，二者缺一不可并加盖投标人公章。

法定代表人或授权代表（签章）：

投标人名称（盖章）：

日期：　年　月　日

6.技术参数响应情况；

特别说明：技术规格书中标注“★”的为实质性条款，负偏离（或未响应）的作废标处理；标注“▲”的为重要条款，每负偏离（或未响应）一项扣 1 分；其余未标注符号的为一般条款，每负偏离（或未响应）一项扣 0.5 分，扣完为止。要求提供佐证材料的条款，若未提供视为负偏离（或未响应）。

7. 认证证书（若有，格式自拟）；

8.人员配备

拟派人员配备情况

序号	姓名	本项目 主要工作	职称/职务	证书名称	专业/ 年限	类似服务的经历、业绩等介绍 （或另附简历）
1						
2						
3						

注：提供人员有效证书复印件及投标人为其缴纳的三个月的社保证明（统一要求 2025 年 10 月-12 月）等，复印件并加盖公章。如同一人拥有多本证书，只按一本计分。

法定代表人或授权代表（签章）：

投标人名称（盖章）：

日期：　年　月　日

9.项目总体服务方案；

10.售后服务；

11.承诺函

承诺函

致（招标人名称）：

我方（投标人名称），作为参与（项目名称）项目投标的投标人，就本次投标郑重作出如下承诺：

一、资质合规承诺

本单位营业执照经营范围包含本项目所须的经营范围，并在有效期内，无被吊销资质的不良记录。

二、安全业绩承诺

近 5 年公司所承担业务外包范围内无 1 人死亡及以上安全生产责任事故（含劳务外包人员）；未被列入安全生产严重失信主体名单（可通过“应急管理部”“信用中国”官方网站查询）。

三、安全管理机构及安全管理人员配置

本单位依据国家相关法律法规，结合业务类型或企业性质，已设置安全生产管理机构或配全配齐专兼职安全管理人员。

四、安全教育承诺

本单位从业人员均具备所从事岗位所需的安全知识和技能，已建立教育培训档案。

五、从业人员承诺

本单位从业人员文化程度均在初中及以上，身体健康无缺陷，年龄均在 18 周岁以上，无超过法定退休年龄的人员进场从事重体力劳动作业；涉及需具备行业认可资格证书的岗位，从业人员已依法取得行业认可的资格证书。

六、劳动合同与工伤保险

本单位已与所有从业人员签订合法有效的劳动合同，并依法为从业人员缴纳养老保险、工伤保险等。结合作业风险情况及自身赔付能力，视情为其从业人员投保第三方人身意外保险。签订合同前提供相应的劳动合同证明及社保缴纳明细。

七、劳动防护用品承诺

本单位为从业人员配备与其作业相匹配的劳动防护用品，且均符合国家标准或行业标准。

八、风险管控承诺

本单位已对承包项目的主要风险进行辨识，并制定了管控措施，建立了风险分级管控清单。

九、设备保障承诺

本单位投入本项目的设备数量、型号与外包业务需求匹配，设备资质及检测情况符合行业标准，设备维护计划可行。

本单位郑重声明：上述承诺内容真实、准确、完整，如有虚假或违反上述承诺，本单位自愿承担由此产生的一切法律责任，包括但不限于取消投标资格、中标资格，解除合同，并赔偿招标人及相关方的全部损失。

特此承诺！

法定代表人或授权代表（签章）：

投标人名称（盖章）：

日期：　年　月　日

12.商务技术标评审所涉及的其他资料（若有，格式自拟）：

13.投标人需要特别说明的其他文件（若有，格式自拟）。

第三部分：资审文件

1. 法定代表人身份证明书或法定代表人授权委托书

法定代表人身份证明书

投标人名称：

单位性质：

地址：

成立时间：　　年　　月　　日

经营期限：

姓名：　　性别：　　年龄：　　职务：

系_____（投标人名称）_____的法定代表人。

特此证明。

附：法定代表人身份证正反面复印件。

投标人（盖公章）：

法定代表人（签章）：

日期：　　年　　月　　日

法定代表人身份证正反面复印件

法定代表人授权委托书

致_____（招标人）：

我（姓名）系（投标人名称）的法定代表人，现授权委托本单位在职职工（姓名）以我方的名义参加_____（项目名称）_____项目的投标活动，并代表我方全权办理针对上述项目的投标、开标、评标、签约等具体事务和签署相关文件。

我方对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（签章）：　　法定代表人（签章）：

职务：　　职务：

被授权人手机号码：

投标人（盖章）：

日期：　年　月　日

授权代表身份证正反面复印件

2. 有效的营业执照扫描件（加盖公章）；

3. 投标人资格声明函

投标人资格声明函

（一）我单位：

1、具有合法有效的营业执照；

2、具有良好的商业信誉和健全的财务会计制度；

3、具有履行合同所必需的设备和专业技术能力；

4、有依法缴纳税收和社会保障资金的良好记录；

5、参加招标投标活动前三年内，在经营活动中没有重大违法记录；

6、法律、行政法规规定的其他条件。

（二）我单位承诺遵守以下要求：

单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不得同时参加同一合同项下的采购活动。除单一来源采购项目外，为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的投标人，不得再参加该采购项目的其他采购活动。

（三）我单位承诺我司具有完成本次招标项目的能力。

（四）我单位非联合体投标。

特此承诺。

法定代表人或授权代表（签章）：

投标人名称（盖章）：

日期：　年　月　日

4. 投标人基本情况表

投标人基本情况表

<table>
<tr><td>投标人名称</td><td colspan="7"></td></tr>
<tr><td>注册地址</td><td colspan="3"></td><td>邮政编码</td><td colspan="2"></td></tr>
<tr><td rowspan="2">联系方式</td><td>联系人</td><td colspan="2"></td><td>电话</td><td colspan="2"></td></tr>
<tr><td>传真</td><td colspan="2"></td><td>邮箱</td><td colspan="2"></td></tr>
<tr><td>法定代表人</td><td>姓名</td><td></td><td>技术职称</td><td></td><td>电话</td><td></td></tr>
<tr><td>成立时间</td><td colspan="2"></td><td colspan="5">员工总人数：</td></tr>
<tr><td>营业执照号</td><td colspan="2"></td><td rowspan="4">其中</td><td>高级职称人员</td><td colspan="2"></td></tr>
<tr><td>注册资金</td><td colspan="2"></td><td>中级职称人员</td><td colspan="2"></td></tr>
<tr><td>开户银行</td><td colspan="2"></td><td>初级职称人员</td><td colspan="2"></td></tr>
<tr><td>账号</td><td colspan="2"></td><td></td><td colspan="2"></td></tr>
<tr><td>经营范围</td><td colspan="7"></td></tr>
<tr><td>财务状况</td><td colspan="7">1、2023 年-2024 年的资产负债情况：
（1）固定资产 _____ _____
（2）流动资产 _____ _____
2、投标人 2023 年到 2024 两年的经会计师事务所审计的年度财务报表，包括资产负债表，现金流量表及损益表。
（1）营业收入 _____ _____
（2）营业利润 _____ _____
（3）利润总额 _____ _____
（4）净利润 _____ _____</td></tr>
<tr><td>备注</td><td colspan="7"></td></tr>
</table>

5. 投标保证金缴纳凭证；

6. 合格投标人的资格要求业绩证明材料（如有）；

7. 招标文件要求的或投标人认为有必要提供的其他情况说明或资质证书（扫描件加盖公章）。