中国人寿保险（海外）股份有限公司

NPAM 监控系统项目

招标清单及技术指标

2023 年 4 月

目　　录

第一章 适用范围

本技术规范书明确中国人寿保险（海外）股份有限公司 NPAM 监控系统项目采购（以下简称：本项目）的基本需求，也是对供应商（以下简称：乙方）的基本要求。通过本文件规范供应商的服务方案设计、实施过程及成果验收交付。

本技术规范书所有内容和技术要求属于安全保密信息，所有参与相关商务投标的供应商不得扩散或者泄露任何相关内容。

第二章 背景、目标及范围

2.1 项目背景

为保障持续稳定的网络流量常态化监测和运营能力，本项目通过建设 NPAM 监控系统，对中国人寿保险（海外）股份有限公司（以下简称“国寿海外”）关键业务节点相关流量进行采集分析，以业务视角将网络性能/主机性能/应用性能做关联一体化分析，实现主动式业务管理，减少网络瘫痪、网络故障和性能下降的时间；优化网络流量，提升关键业务生产力以及增强整体的网络安全防护水平。

2.2 总体目标

根据集团信息化建设数字转型以及未来业务上云计划的目标和需求，针对在云上网络以及传统云下网络中有效监控分析能力方面的优化，为了进一步保障国寿海外网络、系统业务的稳定、安全、高效运行。通过引入基于原始数据包采集分析监测分析系统，实现对全网数据的长期实时监测分析能力，提供更加主动的故障、性能和安全分析功能。

短期目标：传统云下网络流量、业务流量的全时全量监控，实现网络或应用

故障一分钟告警准确率 90%，十分钟故障范围定位 60%

最终目标：云上云下一体化监控完成一五十工程：一分钟故障发现，五分钟根因定位，十分钟恢复。其次，结合智能算法，实现主动智能运维，为网络、应用、业务提供有价值的运维参考数据。

2.2.1 范围概述

根据市场前沿、同行业解决方案、现有 IT 运维的综合调研及分析评估，在网络中重点节点部署监测分析系统，实现更加完善的网络分析能力，以满足国寿海外业务急速扩增带来的多场景以及未来业务上云的综合运维难题。

1. 全面部署。对各个关键的网络节点和网络链路上部署分析设备，实现对重要流量进行有效的监测分析，从而实现对用户的网络行为、服务器的应用服务行为进行监测分析，在此基础上发现异常并进行分析。

2. 监控链路集中分析能力。对多个关键监控节点的网络流量汇集到回溯服务器上，使用回溯分析控制台，对回溯服务器上采集的流量进行监控分析，警报数据的集中收集和展现，从而提高管理效率。

3. 关键业务应用访问质量监测能力。能够对网络中的关键应用的关键通讯质量指标进行实时分析和展现，包括应用流量、网络双方向延时、应用响应延时、丢包/重传数量等；当应用出现缓慢或中断时，能够基于这些通讯质量指标快速诊断问题是网络原因还是应用系统原因。

4. 实时的行为异常监测和告警能力。提供对流量异常、网络行为异常的实时监测功能，能通过多种技术方式对网络流量进行深入的实时分析，如流量实时统计、主机流量实时统计检测、应用定义和流量实时分析、连接层数据统计和检测、通讯特征的监测分析、通讯内容的监测分析等，实现在实时分析的基础上根据实际需要设定异常告警，在出现流量异常时和行为异常是能自动发现，主动告警。

5. 分析系统必须具备数据包级的分析能力，必须能够通过对网络通讯的 7

层协议分析发现异常网络行为的行为特征，系统需提供网络中所有通讯数据包的细化分析能力，从而实现多角度，多层面的分析网络通讯数据，发现异常通讯流量，才能实现全面的异常监测分析能力。

6. 集中的警报监控与管理能力。能够集中收集并展现各网络监控节点流量产生的告警，及时掌握全网的异常情况及异常事件变化趋势，能够帮助用户建立科学有效的警报分析处理流程，确保每一次告警反应的问题能够得到妥善的处理。

7. 系统要具备长期的通讯数据保存分析能力。当系统监测到异常的流量和异常的网络访问行为时，有能力对当时的流量数据报文进行提取和分析，提供进一步分析的依据，这要求系统能够提供对网络流量数据的长期保存功能，当发现问题时，提供一定时间（3-5 天 ）范围内的回溯分析，提供分析取证的依据。

8.系统需具备云上云下一体化监控能力。传统物理网络通过关键路径交换机镜像，云网络通过 Agent 方式获取原始数据，通过构建云上云下网络架构及关联流量数据，实现从广域网、外联、互联网、数据中心核心网络、云网络一体化的云上云下监控能力。

2.2.2 需求概述

本期项目对乙方提供的网络流量回溯分析系统应当具备的基本功能、场景化功能以及安全分析功能需求，概述如下：

序号	功能模块	概况描述
1	软硬件性能	提供设备需满足两个机房关键网络节点流量监控
2	系统架构	系统架构需具备灵活性，满足不同程度用户的使用；针对不同或相同网络节点的识别支持多种方式进行统计分析

3	流量回溯与分析	针对运维场景中流量回溯分析需求，提供不同维度的监控视角，实现不同运维的分析需求；且需支持外部多种数据包格式导入系统进行分析；
4	数据捕获与存储	支持流量去重功能，针对特定的网络节点可设置不同的捕获与存储策略
5	应用监控与分析	支持对任意时段指定关键应用的服务质量分析功能、支持 HTTP 协议、数据库协议、SSL 协议的交易识别、DNS 协议分析功能；支持视频监控/视频会议等基于 Voip 的视频质量分析功能；支持多地数据中心业务的配置下发统一界面监控功能
6	数据包解码分析	系统需具备自主知识产权的数据包解码分析软件，具备智能诊断功能
7	异常流量监测	支持异常流量告警附带 TOP 信息（IP/IP 会话）以及各种维度流量的告警功能，支持指标阈值加持续时间的告警，告警设置可配置为超出阈值或低于阈值，所有告警方式均支持秒级单位告警
8	运维场景监控与分析	支持为组成业务的每个应用集中配置性能监控警报；支持链路流量数据自学习功能；可以选择数据源、站点、应用、输出字段和颗粒度；支持 NAT 前后会话的关联分析能力；支持报表功能；支持第三方平台标准的接口免费对接
9	系统管理与维护	支持审计日志，可记录所有用户对系统的操作信息。设备登录时支持联动 AD 服务器，无需再逐个配置账户密码。

2.3 技术要求明细

2.3.1 基础功能

为更好地满足此次项目设计的流量分发的需求，需满足下表列出的网络回溯系统软硬件设备：

注：标记为★的需求为必须满足项，标记为▲的需求为需截图证明项

产品	数量	配置及参数
流量回溯分析系统 （软件+硬件）	2 套	回溯分析系统专用硬件平台 ★支持冗余电源 ★最大存储：≥48TB ★采集接口：≥4 个千兆光口；≥2 个万兆光口 ★最低流量处理性能≥2Gbps ★CPU 性能：≥XeonE-2286G 6C 4.0GHz ★内存：≥32GB ★含三年维保及技术支持服务。

统一业务性能管理平台 （软件）	1 套	NPAM 集中管理及统一展示平台 ★包含 30 个业务管理授权 ★最高管理 30 台 NPAM 网络流量探针 ★提供三年软件免费升级服务及技术支持服务。
网络分流器 （TAP 硬件）	1 台	★提供电源冗余模块 ★流量处理性能≥480Gbps ★采集接口≥48 个 SFP+接口，且兼容万兆/千兆 ★支持流量复制转发、过滤、负载均衡、报文预处理功能 ★提供三年软件免费升级服务及技术支持服务。

2.3.2 场景功能

功能类别	功能参数
系统架构	▲1、设备同时支持提供 C/S 和 B/S 架构，给用户提供灵活的分析模式，B/S 具备简单主动分析和综合展示能，C/S 架构满足专业用户灵活快速分析定位故障的要求（提供产品功能截图）
	2、支持根据 MAC、VLAN ID、MPLS 标签、VxLAN ID、IP 网段设置虚链路,能够基于虚链路实现性能统计、分析、存储。支持 netflow、netstream、流量分析功能，能够接收 netflow、netstream 流量数据并统计分析

	3、支持云上云下统一监控能力，能够支持云上云下统一监控，兼容传统网络流量分析产品，实现一套平台完成云上云下统一监控及分析，实现异构云全栈式监控分析能力
数据捕获与存储	1、支持 IPv4 以及 IPv6 流量去重功能，能够在原始流量存在重复包的情况下自动剔除重复的数据包，确保分析结果的准确性
	2、支持针对特定的网络节点。根据不同的应用协议设置不同的原始数据包存储策略，至少包括只存储数据包头、完整数据包存储、不存储 3 种方式；数据包的存储方式不影响指标数据的存储，在只存储数据包头或不存储数据包时能够实现指标数据的正确分析与存储。能够自定义的分配存储空间。针对不同网络节点能够对原始数据包，统计数据按照每秒，每分钟，每十分钟，每小时，每天进行灵活存储而不影响历史数据
	▲3、设备支持对流量的指标进行秒级的默认开启自动刷新滚动和展示，且对流量性能具有毫秒级的分析能力（例如：网络五元组，丢包率，重传率，入网数据包数、出网数据包数、全部数据包数）（提供产品功能截图）
	▲4、Agent 流量采集在 2 核、2GB 内存资源下，支持≥5Gbps 流量采集及流量分发能力。（提供产品功能截图）

	▲5、支持通过平台页面统一上传和删除采集 Agent 安装包。支持平台页面统一卸载采集 Agent。（提供产品功能截图）
	▲6、采集 Agent 能够支持资源占用限制，以保证 Agent 资源占用在可控范围，可限制资源保护：CPU 使用核数限制、内存利用率限制、转发速率限制。（提供产品功能截图）
	▲7、Agent 熔断机制，支持对系统整体资源进行监控，如 CPU、内存，当整体负载量较高时，Agent 能够自动熔断停止工作，优先保证业务能够有足够资源运行，同时发出告警。（提供产品功能截图）
	▲8、Agent 自我监控模式，当在极端情况下分析中心与 Agent 中断后，仍能保持对系统状态的监控，资源限制及负载保护机制任然能运行；当宿主资源状态恢复到正常值时，能够自动恢复采集。 当中心与 Agent 通讯断连的情况下，以上能力依然生效。（提供产品功能截图）
流量回溯与分析	▲1、支持对单个主机的流量进行回溯分析，能够提供单个主机的流量趋势图，可分析指标＞100 个，分析指标包括但不限于：总字节数（区分接收、发送字节数）、总数据包数（区分接收、发送数据包数）、字节收发比、数据包收发比、平均包长（区分接收、发送平均包长）、请求最大传输时间、响应平均传输时间、响应最大传输时间、平均空闲时间、最大空闲时间、最小空闲时间，所有统计指标支持 1 秒

	级时间精度刷新与呈现；分析界面支持按任意指标值升序、降序排列；能够区分识别内、外网主机信息，并能够通过 API 方式对接国寿 CMDB 获取 IP 名字表，互联网 IP 能够识别运营商归属信息。要求分析的 IP 主机 TOP 排名达到 30 万条以上且所有统计指标支持实时 1 秒时间精度存储与呈现。支持任意界面下模糊检索（提供产品功能截图）
	2、支持对 IP 会话的流量进行回溯分析，能够提供单个 IP 会话对的流量趋势图,可分析指标＞100 个，分析指标至少包括：TCP 重传包、TCP 分段丢失包、TCP 重复确认包、三次握手次数、三次握手平均时间、TCP 有效载荷数据包数、TCP 乱序包数、传输效率、平均窗口大小等性能指标；所有统计指标支持默认自动开启秒级精度的刷新和趋势展示；分析界面支持按任意指标排序。要求分析的 IP 会话 TOP 排名达到 30 万条以上且所有统计指标支持实时 1 秒时间精度存储与呈现。支持任意界面下模糊检索
	3、支持对 TCP 会话的流量进行回溯分析，能够提供单个 TCP 会话的流量趋势图，可分析指标＞100 个，分析指标至少包括：客户端/服务器地理位置、会话开始/结束/持续时间、客户端/服务器负载数据包数、客户端/服务器 TCP 分段丢失包、平均/最大响应时间、总响应时间、客户端请求总传输时间、服务器响应总传输时间、首次响应时延、建链成功率、建链成功数、客户端/服务器平均 ACK 时延等指标；所有统计指标支持默认自动开启秒级精度的刷新和趋势展示；分析界面支持按任意指标排序。要求分析的 TCP 会话 TOP 排名达到 30 万条以上且所有统

	计指标支持实时 1 秒时间精度存储与呈现。支持任意界面下模糊检索
	4、数据特征值回查，能够通过数据流任意数内容进行回查，提供数据包导出界面，能够选择时间、应用、站点、Vxlan、Opcode、协议类型、以太网协议、IP 地址、端口等信息进行过滤导出，并提取相关的数据包且回查结果精确至纳秒级别
	▲5、支持利用服务器 IP 地址、协议端口号、协议端口号范围、客户端 IP 地址、客户端端口范围等条件，自定义组合应用。支持使用 URL 路径自定义应用。支持使用特征值定义应用。支持使用协议定义应用且要求协议支持 1000 种以上。支持基于未知流量的统计、快捷定义未知应用。支持区分短连接、长连接、异步长连接（提供产品功能截图及第三方报告证明协议支持 1000 种以上）
	6、支持数据包回放功能，能够将通过其他方式获取到的数据包导入系统进行分析（无需其他组件播放），页面至少支持 3GB 数据包回放，实现与实时采集链路相同的分析功能，数据包格式应包括 sniffer、tcpdump、wireshark 等抓包软件常用格式，例如：cap、pcap、rapkt、cscpkt、rawpkt、5vw、pkt、TRC0、TRC1、trl、pcapng、pcapng.gz、ntar,ntar.gz、Snoop 等

	▲7、展示界面支持 SRv6 协议 TCP 会话统计，能够自动获取 SRv6 段列表信息，自动梳理出会话双方向访问路径中经过的网络设备，并提供梳理结果视图。（提供产品功能截图）
	▲8、支持无线流量分析功能，自定义 CAPWAP 特征，可将集中转发模式下的无线隧道进行剥离分析，达到识别实际无线终端数据流量分析（提供产品功能截图）
应用监控与分析	1、支持对任意时段指定关键应用的服务质量进行分析，服务质量指标包括：TCP 连接请求无响应次数、TCP 连接请求被重置次数、上行/下行 TCP 分段丢失包、上行/下行 TCP 分段丢失率、上行/下行传输效率、三次握手平均/最大/最小时间、TCP 交易总数、TCP 交易无响应次数/无响应率、平均/最大首次响应时延、平均/最大用户响应时间、客户端/服务器平均重传时延、好/一般/差/响应超时的 TCP 交易次数，所有统计指标支持默认自动开启秒级精度的刷新和趋势展示；分析界面支持按任意指标排序。
	2、支持 HTTP 协议的交易自动识别功能，提供交易处理数量、响应统计、交易处理时间趋势图，能够统计每个 URL 的流量、请求次数、响应次数、无响应次数、请求传输时间、响应传输时间、交易处理时间、HTTP 响应状态码等交易统计参数，支持对交易内容进行分析，所有统计指标支持默认自动开启秒级精度的存储和趋势展示；分析界面支持按任意指标排序。

	3、支持 Oracle、SqlServer、MySQL 协议的交易识别分析功能，提供交易、端口号、功能号处理数量、响应统计、交易处理时间趋势图，能够统计每个 SQL 语句的请求/响应/无响应次数、请求传输时间、响应传输时间、交易处理时间等交易统计参数以及功能号基线性能比对。
	4、支持 HTTP 协议使用 URL 路径自定义应用。支持使用特征值定义应用。并且该协议全部指标参数支持按 1 秒级时间精度刷新展示和分析。能单独对一条 URL 的流量进行多维度分析。指标包含且不限于流量，总字节数，响应字节数，请求字节数，比特率，数据包数，好/一般/差/等详细指标
	5、产品支持下发配置信息以及集中监控、分析和管理。要求产品数据接口输出比特率、峰值流量、总字节数、总数据包、会话总数、创建会话数、关闭会话数、每秒活动会话数、好/一般/差的 TCP 交易次数等指标。支持多地数据中心部署的业务能够直接在同一界面进行梳理展示，无需二次开发。
	▲6、全面支持视频监控/视频会议等基于 Voip 的视频质量分析，能够识别基于 RTP 协议的通讯流量，能够对 H.323、H.264 等分析，支持快速统计、展示出选中时间段（1 秒级精度）内的总流量、峰值流量、呼叫数量、呼叫时长、视频最大 MoS、视频平均 MoS、视频最小 MoS 等（提供产品功能截图）
	7、支持下发配置信息以及数据的集中监控与分析。

	集中监控业务做统一全节点集中可视化监控。服务质量指标包含并不限于如下几点：（TCP 连接请求无响应次数、TCP 连接请求被重置次数、上行/下行 TCP 分段丢失包、上行/下行 TCP 分段丢失率、上行/下行传输效率、三次握手平均/最大/最小时间、TCP 交易总数、TCP 交易无响应次数/无响应率、平均/最大首次响应时延、平均/最大用户响应时间）
	▲8、无需手工自定义应用配置，能够自动识别云网内 WEB 应用（HTTP 基于 HOST 自动识别，自动进行应用流量可视化及智能监控告警，实现开箱即用的应用监控（提供产品功能截图）
数据包解码分析	▲1、系统内置自主知识产权的数据包解码分析软件，并能识别 SRv6 协议，识别 SRH 扩展信息，提供计算机软件著作权登记证书，支持在任意分析界面直接提取原始数据包进行解码分析。（提供产品功能截图以及相关证书）
	▲2、解码软件具备智能诊断功能，能自动诊断包括：HTTP 错误、SMTP/POP3 服务器慢响应、SMTP/POP3 服务器返回错误、FTP 服务器慢响应、FTP 服务器错误、TCP 连接被拒绝、TCP 非法校验和、TCP 重复的连接尝试、DNS 错误、会话连接故障、重传、IP TTL 大小、IP 地址冲突等常见故障场景，并提供故障原因分析及解决办法。解码软件必须支持中文操作界面，数据包解码分析所有功能项目要求数据包解码字段包括数据链路层头部、IP 头部、TCP\UDP 头部等字段及选项解码必须支持中文显示。（提供产品功能截图）

运维场景监控与分析	1、支持为组成业务的每个应用集中配置性能监控警报，警报触发条件应包括采集前端设备所支持的所有应用性能监控参数，并支持通过与、或、非等逻辑关键进行多参数组合报警，警报触发时间间隔可定义 1 秒、10 秒、1 分钟，支持定义警报抑制阈值，警报报警参数需大于 60 种。
	2、支持链路流量数据自学习功能，能够根据链路历史数据对链路未来趋势进行预测，支持按天或按周进行趋势分析，支持设置未来趋势的天数，支持趋势预测的指标包括：比特率、指标。
	3、系统对流量中对全部统计指标包含（峰值流量、总字节数、异常 IP 流量、非 IP 总流量、总数据包、会话总数）等指标均支持默认自动开启秒级精度的刷新和趋势展示，支持自动化故障定位，能够对业务路径中各组件的指标及告警做关联分析，自动判断出产生告警的根源组件。
	▲4、支持毫秒级自动分析，精度 1ms 的统计分析。支持 1 秒精度指标曲线绘制，毫秒精度链路流量构成分析。默认开启并自动以 1s 精度向前滚动。（提供产品功能截图）
	▲5、设备支持在无需对接第三方日志的前提下进行 NAT 前后会话的关联分析能力，在 IP 会话源地址目的地址转换的前提下，通过单边 IP 会话能自动检索出源目转换以后的 IP 会话信息并能在统一界面分析数据包详细指标信息。（提供产品功能截图）

	6、设备支持报表功能，能自定义 IP 地址、网段、业务、应用、单独的 URL 进行各项指标的数据分析。且支持不同站点同时分析的能力。提供扩容报表，可选中某链路的所有站点，设置利用率的阈值，统计每个站点超过该利用率的连续天数和总天数。
	▲7.支持业务调用链多个应用节点出现告警时，自动根据事件类型智能推导根因节点定位，并高亮或明显标识异常根因节点。（提供产品功能截图）
	▲8、支持告警恢复功能，当告警产生时，持续监控系统状态，当系统恢复正常 KPI 水平时告警自动消除，并提示监控对象恢复正常（提供产品功能截图）
	▲9、支持自动关联分析每条告警关联的应用性能指标趋势与网络性能指标趋势，包括但不限于：请求量、响应量、成功量、总响应时间、字节数、比特率、包数量、会话总量、创建会话量、活动会话量、建连成功率、重传率、丢包率、三次握手次数、连接请求总数、连接失败次数、连接建立重置次数、连接建立无响应次数、三次握手平均 RTT、SYN 包数、SYN/ACK 包数、FIN 包数、RESET 包数（提供产品功能截图）
	▲10、支持对云上监控的应用、资产一键开启动态基线学习功能，无需手工设定阈值及基线偏离上线偏离度即可实现动态基线告警能力；支持基线指标包含：

	请求量、响应量、成功量、总响应时间、字节数、比特率、包数量、会话总量、创建会话量、活动会话量、建连成功率、重传率、丢包率、三次握手次数、连接请求总数、连接失败次数、连接建立重置次数、连接建立无响应次数、三次握手平均 RTT、SYN/ACK 包数、FIN 包数、RESET 包数。（提供产品功能截图）

2.3.3 安全及异常分析功能

功能类别	功能参数
异常流量监测	1、支持对未知流量得监控，可以通过自定义流量中的会话数、连接数等定义安全告警以及数据包中的特征、HEX 码、ASCII 码、XFF 字段等自定义安全告警（所有告警需要可以通过逻辑字符进行组合同时告警需要携带 TOP 信息）
	2、支持对异常行为的监控，可以通过异常的行为看到异常的类型，支持异常行为主机与其它主机/服务器交互情况，支持异常 IP 感染和导致失陷服务器/主机，支持异常特征、IP、等信息的导入
	▲3、支持告警状态智能升级及转化： 能够对告警进行自动化事件升级，如当多个风险级别告警存在事件关联时，自动升级为故障或事故级别告警事件 支持告警中、告警恢复状态自动转化，当业务出现突发告警时，告警状态为“告警中”；当业务恢复正

	常 KPI 水平时，告警状态自动转化为“恢复”。（提供产品功能截图）
	▲4、支持告警管理生命周期记录，包括首次触发、最后触发、告警响应、告警恢复、告警关闭、告警评估关键里程碑及处理流程可视化（提供产品功能截图）
	▲5、支持多种告警聚合模式，减少告警处置疲劳，支持模式包含： 基于告警对象进行告警事件聚合 基于告警对象+单指标进行告警聚合 基于告警对象+事件进行告警聚合（多指标组合） （提供产品功能截图）
	▲6、支持五个告警级别：事故、故障、告警、风险信息、恢复，从而给用户直观的处置重点。（提供产品功能截图）

2.4 非功能需求

2.4.1 原厂综合实力要求

为了展示原厂自身综合实力：需提供原厂注册资金证明，NPAM 国内市场占有率排名报告及原厂产品获得的国际评价证明（如无可不提交）

为了更好的证明公司综合实力以及满足一些公共标准原厂尽可能具备例如（ISO9001 质量管理体系认证、ISO14001 环境管理体系认证证书、信息安全服务

资质、CMMI 能力成熟度模型（3 级及以上）、Gartner 魔力象限进入报告证明、业务连续性管理体系等同类资质）

投标人认为还有其他需要提供的原厂实力证明资料；

2.4.2 非功能需求项要求

为保证产品在性能以及适用性需求，原厂本次投标产品尽可能具备以下非功能需求资质例如（IPv6 Ready 认证、CSTC 中国软件评测中心鉴定报告对协议支持能力达到 1000 种以上相关证明、中国国家信息安全产品认证、信息技术产品安全测评证书同类资质证书）

针对未来业务上云计划，原厂资质需保证支持多类型云，至少包含主流云平台的适配，如：腾讯云、阿里云、华为云、百度云（提供资质认证材料）

第三章 项目实施说明

本项目，分为项目调研和需求分析、系统部署与调试、系统上线阶段、项目总结及上线后运维移交阶段。乙方各阶段所执行的主要工作任务和内容包括但不限于如下：现状调研

3.1 项目调研和需求分析

- ➢ 项目启动会议，建立项目计划；
- ➢ 系统环境及外围系统关联性调研；
- ➢ 软、硬件资源的建议及项目各项需求的建议。

3.2 系统部署、调试、对接

➢ 按照甲方流程进行调试；

➢ 妥善处理调试部署后的各种问题。

➢ 按照甲方要求乙方产品配置业务系统监控（例如 OA、开门红等）。

3.3 系统上线

➢ 按照甲方流程进行系统上线；

➢ 对系统上线后的使用问题进行跟踪排查；

➢ 对系统进行优化调整。

3.4 运维移交

➢ 对项目进行总结，整理并交付所有要求的项目文档、技术材料；

➢ 建立针对所部属内容的安装、配置、监控、巡检、日常运维、应急 等运维体系；

➢ 出具功能方面的成果报告；

➢ 安排本项目的知识转移；

➢ 对于由乙方在项目实施过程中负责部署的内容，如果在部署后出现问题，由乙方负责进行解决。

第四章 项目管理

4.1 项目管理方法论

乙方须依据自身的项目管理方法论，结合国寿海外项目实际情况，提出合理优化的适应本项目的项目管理方法论，并在项目实施过程中,包括项目启动、执行与控制、收尾等阶段贯彻执行。

4.2 项目实施组织

为保证维保服务的顺利实施，乙方应根据项目实施要求派驻足够的人员到甲方现场进行项目实施，并且在现场期间遵守甲方的工作纪律和要求。同时，甲方根据项目实施需要，组织相关人员参加此项目，与乙方人员紧密结合成项目实施小组。

乙方应提出详细的实施组织建议。项目实施组织的具体形式、人员组成及分工由双方在项目启动阶段根据项目实施需要协商决定，并报甲方批准执行。在具体项目实施各阶段，可根据需要，提出项目实施组织或/和人员组成变更申请，经甲方批准执行。

4.3 项目实施人员要求

投标方必须在投标文件中列出参与项目的项目总监、项目经理、主要顾问、专家的资历、投入本项目的时间及在本项目承担的职责。

中标方投入的项目主要成员必须和投标文件中建议的人员一致，未经招标方同意，不允许更换（人员离职或健康原因等特殊情况除外）。

4.4 项目驻场人员需求

为满足用户日常运维和异常或故障情况下的及时响应,原厂深圳技术团队人员以及原厂驻场人员需满足以下需求：

驻场人员需为原厂人员且必须具备网络流量分析相关资质证书（须提供工程师公司归属证明材料复印件加盖章(归属证明材料形可为公司承诺函、员工证或

雇合同)。 如提供的是子公司证书的，须提供公司隶属关系证明材料复印件，提供驻场员工社保 6 个月缴费清单）

除驻点人员外，原厂深圳需常备 10 人以上的技术团队以备相关技术答疑以及重要活动保障支持；需提供 6 个月以上社保证明（须提供工程师公司归属证明材料复印件加盖章(归属证明材料形可为公司承诺函、员工证或雇合同)。 如提供的是子公司证书的，须提供公司隶属关系证明材料复印件，提供社保 6 个月缴费清单）

驻场人员日常工作内容如下（包含但不包括）:

1. 负责协助处理生产网络运维工作,包括路由交换、防火墙、负载均衡、VPN、波分及其他网络安全设备、专线等通过本次投标设备的日常检查和运维，对上述设备进行网络分析服务：主动完成日常监控、隐患排查、故障分析、故障处理等日常监控、隐患排查、故障分析、故障处理的提供帮助。
2. 通过本次投标设备协助处理生产网络建设项目实施的支持和保障工作
3. 通过本次投标设备协助处理生产网新业务系统上线的支持和保障工作。
4. 协助处理生产网络巡检及监控处理、故障处理、变更管理、专线管理等运维工作。
5. 协助完成领导安排的其他工作。

4.5 项目实施计划

本项目中，乙方需要按照国寿海外要求的时间点安排实施计划，按时完成项目相应内容。

4.6 项目质量管理

质量控制队伍应该独立于项目组，作为项目成功的重要因素和保障，在项目执行过程中始终与项目组保持密切联系。从另一个角度观察和监督项目的开展，帮助项目组发现和解决项目执行中的问题，确保项目的成功。

在组织结构上，将设置质量控制小组，专门负责项目实施的质量控制。质量控制小组由项目双方项目经理、业务人员及双方领导组成，乙方专门指定一位高级经理作为质量总监。

质量管理小组将定期或不定期的举行检查会议，进行项目各阶段提交件的评审，听取项目经理及项目其他人员的汇报，对项目的进展和质量进行监督和控制，提出有关建议和意见。

质量管理小组的每次会议的内容，结论和决定，都将形成文字备忘录，为项目文档保存，并作为以后工作的依据，随时对项目的进展和质量进行修正。

第五章 供应商责任

供应商须确认并承诺能够完成本技术规范中所要求的需求内容以及按要求组织项目团队，确认并承诺承担本技术规范书中所要求供应商承担的所有责任，不满足。

要求本次所投产品的技术参数需求项需当前版本满足，不接受中标后版本升级迭代满足。招标人在发放中标通知书之前，可视情况设置测试验证环节，投标人需在规定时间内提供测试设备进行功能验证，如有厂商技术参数虚假应标将会被永久拉入国寿海外供应商黑名单，后续不能参与国寿海外所有项目。

5.1 供应商组织要求

为保障项目以及产品落地成功，同时为了确保乙方提供的技术服务响应的及时性、有效性。要求乙方具备本地团队，提供本次项目团队主要成员简历； 乙方提供最近半年的社保缴纳证明供应商职责要求

5.2 供应商职责要求

供应商须对项目的全部内容进行应答，按照本技术规范要求提交全部资料，并对本技术规范各方面做出实质性响应（确认或提出异议）。

1）对本项目范围、内容、所承担的任务的理解与确认；

2）本项目管理方案建议包括但不限于：

➢ 设计项目组织结构，明确双方职责和主要任务；

➢ 详细工作进度计划/策略，包括对工时、人力、费用等资源需求的预 期；

➢ 拟提交成果清单及说明；

➢ 培训方案；

➢ 项目人员简历及资质证明；

➢ 项目验收标准；

➢ 项目实施经验；

➢ 项目实施组织、工作职责。

第六章 培训与知识转移

在项目中，为确保项目的可持续性发展，保证从设计阶段到实施阶段和上线维护的平滑过渡，以及降低不同阶段过渡过程的不确定性和可能的执行偏差，通过多种方式提供项目技术培训。

知识转移是将专家的特定能力转移到项目组的客户成员，并最终转移到客户整个组织。根据本次项目总体内容和时间进度要求，乙方安排有关项目方法、项目成果等方面的培训,相关知识培训内容包括：

6.1 培训要求

1）在项目启动时，向项目组进行产品使用培训；

2）在项目实施过程中，通过技术培训、人员访谈、数据收集、分析整理、研讨会等形式向项目组进行知识转移。

3）在项目实施结束前，向项目组进行产品维护培训；

4）应提供中文培训资料、讲义、模板等资料。

第七章 项目交付与成果物

7.1 项目成果交付

为了确保项目实施的成功，在项目中的各级交付文件非常重要，乙方需要按照双方约定的格式提交项目相关文档。

为确保项目按照项目预期的计划执行，在项目实施过程中，一些重要文件需要国寿海外项目经理或相关人员进行审批和确认。

在项目各阶段交付物内容与要求（包含但不限于以下内容）：

- 项目实施计划
- 项目实施方案
- 项目调研提纲及调研结果
- 培训计划及资料、讲义、模板
- 其他增值服务记录（如有）
- 项目总结报告
- 工作遗留项及关注事项

7.2 售后服务

乙方在项目验收后 6 个月内依据实际情况提供不少于 5 次的电话指导、邮件指导或远程支持，每次支持时间在半天以内。

在服务结束后一年内，将至少回访国寿海外 2 次，对国寿海外网络安全软件系统和硬件设备的现状做了解和访谈，并提出针对性建议。

第八章 验收

本项目的验收标准为：乙方完成 NPAM 监控系统平台的建设工作，完成场景功能的实施，确保所建设的平台满足非功能要求，平台平稳运行，完成项目成果交付以及知识移交。

符合验收标准后，乙方须提前十四天用书面方式向国寿海外提出验收申请，由国寿海外组织项目验收小组对项目成果物进行验收，如验收通过，则由国寿海外出具最终验收证书。

上述各验收阶段均与付款直接相关，具体条款经甲乙双方商定后，体现在具体合同文本中。