四川省生态环境保护信息安全保障体系项目技术方案

一、项目概述

四川省环境信息中心作为四川省生态环境厅直属单位，承担了省厅网络信息安全管理与维护等基础保障工作。通过采购信息安全体系安全运维服务切实保障网络和信息系统的可用性、安全策略的连续性，有效地防范信息安全突发事件，确保四川省生态环境厅信息基础设施和系统能够安全、稳定、高效运行，做到无重大信息安全事故发生。

二、项目背景

2025 年四川省环境信息中心采购了信息安全运维服务，切实保障省厅网络和信息系统的可用性、安全策略的连续性，防范信息安全突发事件，确保四川省生态环境厅关键信息基础设施能够安全、稳定、高效运行，该服务将于 2026 年 5 月 31 日到期。2026 年，在四川省生态环境厅现有信息安全体系基础上，继续通过网络安全基础运维保障服务，包括日常运维、应急响应、人员驻场等，全方位保障生态环境厅网络和信息安全，形成更系统、融合、智能的安全保障体系，继续保障厅网络和信息安全可靠，防范信息安全突发事件，确保省厅网络和信息安全无重大信息安全事故发生。

三、服务期限

服务期为 2026 年 6 月 1 日至 2027 年 4 月 30 日。

四、项目技术及服务要求

1.信息安全日常运维服务

设立四川省环境信息安全日常运维小组。

（1）日常服务热线

提供 7×24 小时的安全运维日常服务热线电话，并提供专职人员负责及时受理和响应四川省生态环境厅日常安全运维工作中出现的需求，并对服务需求和响应措施做好详细记录。

（2）日常安全巡检

通过对四川省生态环境厅的安全设备定期进行安全巡检，全面掌控安全设备的运行状态、故障告警等信息，及时进行分析处理，保障安全设备的稳定、可靠运行。

巡检内容主要包括：安全设备的功能模块、硬件状态、设备配置、特征库升级、日志报警等，整体网络的连通性、网络时延、异常流量、异常连接等。

安全巡检每月执行一次，要求备份所有安全设备的配置，并提交月巡检报告和相关处理记录。

（3）安全技术支持

安全运维小组需要对四川省生态环境厅所有的安全设备进行网络安全相关的日常维护工作,本次项目需按照采购人需求和岗位要求提供不少于五人的信息安全技术支持服务,其中包含驻场人员2名且驻场人员需在工作时间常驻四川省环境信息中心办公室。安全运维工作应按流程做好运维过程记录。技术支持工作包括但不限于:日常的安全设备维护、安全策略优化、网络优化改造、网络故障排查、安全状况监控、安全预警通告、安全咨询建议等。

1)安全设备维护。需对以下安全设备(根据采购人实际需求变化进行调整)进行维护,包含但不限于巡检、定期检查设备运行状态、特征库、病毒库是否正常安全配置、设备版本维护升级、特征库和规则库升级、安全设备资产清理等。发现问题及时处理,确保安全设备正常运行,保障生态环境厅网络安全。

序号	设备名称	数量	制造商家
1	防火墙	10	华三、启明星辰、迪普
2	入侵防御系统	2	迪普
3	堡垒机	1	网御星云

2)安全策略优化。包含无效策略清理、策略严密性梳理、策略可读性修正等。

3)网络优化改造。协助采购人进行网络链路维护、优化、改造及拓扑图整理。

4)网络故障排查。协助采购人解决网络中疑难故障。

5)安全状况监控。利用好四川省生态环境厅现有的防火墙、入侵防御系统、堡垒机等安全设施,监控和审计网络运行状况,及时发现网络安全威胁。

6)安全风险排查。按照采购人需求,对四川省生态环境厅业务系统开展安全风险隐患排查,包括漏洞扫描、弱口令扫描和渗透测试,并将扫描结果下发给相关责任单位进行修复,跟踪汇总修复情况。协助软硬件厂商消除弱口令,修复漏洞。

7)安全预警通告。根据环境信息系统的类型及行业特点,定期收集发布相关安全漏洞、安全威胁、业界相关安全事件的情况,及时掌握系统安全风险情况,指导开展安全管理工作。

8)安全咨询建议。为采购人提供网络安全体系、等级保护、数据安全、密码应用等安全相关咨询建议,为日常的网络平台和信息系统建设提出专业的安全意见,协助采购人建立并持续完善网络及数据安全保护体系、制度等。

9)目前省厅业务系统已迁移至政务云,协助采购人对云服务商提供的安全能力进行技术监督,对云服务商日常安全运维工作情况(漏洞扫描、日常安全策略开通、配置备份、重大保障等)进行实时跟进、技术指导,督促云服务商做好

政务云业务系统的日常安全防护工作，保障业务系统安全稳定运行。

（4）驻场服务

★按照采购人工作需求和人员要求提供驻场服务，驻场人员不低于2人，其中安全专家1名。驻场人员需完成采购人安排的工作，并纳入采购人内部管理制度统一管理，服从采购人值班安排（含夜间值班和节假日值班值守），驻场人员值班费、加班费、餐旅费等均包含在本次报价内。**供应商需提供书面承诺函，格式自拟**。

驻场人员需具备以下能力：

1）熟悉各类常见安全设备（FW\IPS\IDS\ATP\WAF\SOC\审计等）工作原理，能独立熟练配置各大厂商安全设备。

2）熟悉路由/交换技术，能独立进行主流厂商设备配置（华为、华三、锐捷等），能独立进行网络故障分析处理。

3）熟悉各类操作系统、熟悉主流虚拟化平台；能独立进行日常维护操作。

4）熟悉常用的各类数据库，能对数据库进行简单的日常维护操作。

5）熟悉各类常见网络攻击原理，能对安全设备的日志进行分析，排查网络中的攻击行为。

6）熟悉各类安全情报渠道，具备将安全情报转化为安全保障措施的能力。

7）熟悉网络安全领域各类（包括但不限于网络安全体系、等级保护、数据安全、密码应用等）政策、法律法规、管理及技术要求，具备网络安全相关文档的处理编写能力。

8）有较强的沟通协调能力和统筹能力，和采购人能够进行顺畅有效沟通，能及时理解采购人交办任务的要求和重点，工作态度端正，责任心强，工作耐心仔细。

2.信息安全应急响应服务

为四川省生态环境厅负责的基础信息平台和重要信息系统发生安全事件时提供应急处理服务，为加强四川省生态环境厅信息安全突发事件的应急管理能力提供应急演练服务，重大活动及节假日应提供应急保障服务。

（1）应急事件处理

提供应急事件处理服务，及时分析处理安全突发事件，阻止攻击源，排除故障，及时恢复网络和业务系统。对安全突发事件按事件级别迅速启动应急预案，了解安全突发事件的基本现象，判断安全突发事件的原因，并进行安全突发事件的处理，协助采购人进行灾难恢复、入侵追踪和证据取证等工作。

序号	分类	细项

1	事故通报	根据事故严重程度级别，进行事件通报
2	事故预处理	事故现场保存、紧急恢复
3	故障排除	实施应急响应预案，开展故障排除工作，及时恢复业务
4	业务持续跟踪	根据需求，持续跟踪观察业务运行情况，保障业务正常运行
5	总结归档	入侵取证、灾难恢复、原因分析、经验教训总结、存档记录

（2）应急演练

协助采购人进行有针对性的应急培训和安全演练，对重要岗位人员培训应急知识和技能，模拟各种可能出现的安全突发事件，发现和验证防护体系的安全性和可靠性，检查队伍的应急配合和反应能力，服务期间内每年须组织两次应急演练。

（3）重大活动及节假日保障

春节、五一、国庆、元旦等节假日及重大政治活动日期间（节假日前后一段时期，根据具体情况而定），以及在国省级安全演练期间，对四川省生态环境厅网络和信息系统进行重点关注，提升应急响应级别，提供全面的安全运维和设备保障服务。

1）技术支持方式包括：现场支持、远程支持。

2）建立双方联络机制。

3）提供整体安全保障方案，内容至少包括：人员配备及分工情况、安全突发事件处理流程、各类安全突发事件处理方法、仪表及工具配备情况等。

4）事件升级机制：安全技术保障人员须具备较强的应急处理能力、较强的安全攻防能力、较强的协调能力。该人员通过一段时间调研后应迅速熟悉掌握四川省生态环境厅网络和信息系统情况、安全设备部署情况，在遭遇安全突发事件时能及时判断事件类型及原因、采取措施保障业务连续性、保存好相关日志等重要信息，以备后续追查等。

5）针对国省级各类安全演练活动，除上述保障支撑外，还需按需临时提供保障设备或保障工具进行支撑。做好互联网暴露面排查、资产梳理、安全设备策略配置优化、漏洞弱口令风险排查等准备工作，统筹组织整体防守，进行实时监测分析，第一时间发现安全威胁，分析研判攻击造成的危害和影响，准确有效甄别疑似和真实失陷事件，对攻击事件进行溯源，还原完整攻击路径，形成有效证据材料。

3.态势感知安全平台服务

为保障安全服务工作的可视、可管、可量化，能第一时间了解网络安全态势，对安全数据进行融合分析及呈现，实现态势感知，提高安全监测水平及安全服务工作效率，并能对日志数据进行集中化的搜集、存储，满足网络安全法及等保需求。在服务期内，投标人应针对本项目安全服务提供统一态势感知安全平台服务。

（1）态势感知系统

态势感知平台采用大数据技术，针对高速信息进行采集，融合多源异构数据，实现异构海量安全数据的高效可靠存储，以安全数据为驱动，智能化关联分析技术和基于机器学习的威胁狩猎功能，支撑并实现整体安全状态的可视化呈现，收集纳管各设备告警日志，在此基础上对数据进行综合处理和关联分析，为四川省生态环境厅展示面向全网业务资产防护的安全态势，帮助感知隐患和威胁，进而为安全运维提供决策支撑。

1）日志数据汇聚:支持同时收集多个种类的网络安全产品日志，对各类网络安全产品产生的网络日志、告警日志、系统日志等进行统一收集、存储、范化、富化等操作，为安全预警分析提供数据来源与基础。

①支持对网络设备、安全设备、主机系统的日志、网络流量等多种数据源的采集；支持对日志采集器进行采集配置并下发；提供 Syslog、SNMP Trap、等多种采集方式；并支持数据源信息导入、导出、数据源迁移操作。

②预置支持≥700 种设备进行日志解析，支持统计展示已接入设备总数、日志源的总数及其中在线和离线数量。

③预置日志解析规则≥2200 条，支持对已适配的第三方日志源自动识别并匹配解析策略，无需手动配置即可自动完成数据解析和接入。

④支持一键对未能解析的日志自动生成解析策略，从而快速完成全新日志源的接入。

⑤支持网络空间测绘，支持主动发现网络中的各类资产的 IP 地址、资产类型、资产属性（PC、服务器）等。

2）安全威胁分析:通过对预处理后的海量数据的实时和历史分析，结合多种分析方法，包括关联分析、聚合降噪、机器学习、统计分析、恶意代码分析等多种分析手段对数据进行综合关联，完成网络安全威胁监测分析。

①支持对 SQL 注入、文件上传、目录遍历、勒索软件、软控木马、僵尸网络、网络蠕虫、信息漏洞、漏洞扫描、APT 攻击、暴力破解、HTTP 代理等攻击行为进行检测。**（提供第三方机构出具的具备 CMA 标识的检测报告证明材料）**

②支持对漏洞进行检测，支持检测 IT 设备、应用系统的安全漏洞。支持采用安全检测机制，防止漏洞检测造成被检测 IT 设备、应用系统的宕机、重启等故障。

③支持对弱口令进行检测，支持检测态势感知系统监测范围内的设备、应用系统存在的弱口令，支持检测操作系统远程桌面应用的弱口令，支持检测 SQL Server、MySQL、Oracle 等常用的数据库系统的弱口令。支持采用安全检测机制，防止因弱口令检测造成被检测 IT 设备、应用系统的锁定故障。**（提供第三方机构出具的具备 CMA 标识的检测报告证明材料）**

④支持独立的告警分析功能，该功能至少具备攻击者分析（含外部攻击者、内部攻击者）、失陷情报分析、挖矿木马分析、勒索软件分析、ATT&CK 分析等告警分析能力。

⑤支持对业务安全风险分析，包括未授权登录、越权访问、频繁访问、跨区域访问等。

⑥支持对告警信息的智能排序，实现对告警的优先级做分类，能够清晰展示需要被关注的告警信息。

3）处置响应:通过手工或自动化的方式，阻止现有威胁和紧急威胁。

①支持对威胁告警和安全事件新增自动化响应策略，支持图形化连线拖拽交互的策略设置方式。

②预置支持联动对接多种设备类型，包括且不限于以下类型：终端防护软件 EDR、防火墙、入侵防御系统等。

4）展示呈现:支持对海量数据的原始数据、分析结果数据等数据进行可视化大屏展示，提供人机交互界面，向安全管理人员呈现全方位安全状态。

①支持综合安全态势展示，展示内容包括综合风险分值、安全事件数量、资产脆弱性数量、安全威胁数量、日志数量、威胁趋势变化等，能够从多个维度体现安全态势情况。

②支持告警实时监控态势展示，展示内容包括告警总数量、待处置数量、已处置数量、告警变化趋势、实时告警列表等内容，能够从多个维度体现告警的实时情况。

★5）投标人需提供 1 套态势感知系统服务工具硬件配置要求如下:CPU ≥2 颗 32 核，内存≥256GB，系统盘 ≥960G SSD（Raid 1），数据盘≥48TB，千兆端口≥4 个，万兆端口≥2 个。**(实质性要求，提供相应承诺函)**

（2）态势感知探针

态势感知系统需从网络中采集网络安全基础数据信息，包括流信息、攻击日志、告警事件等。投标人需提供 2 台态势感知探针，通过探针制定规则采集网络信息数据，同时具备深度包解析、双向检测、全流量分析、流行为学习模型、攻击链还原、多维度资产分析等功能，通过与态势感知系统的无缝对接，给上层的态势感知系统提供基础的数据。

★1）硬件参数:内存≥32G、硬盘≥4T，配置≥4个千兆电口，≥2个万兆光口，≥2个扩展插槽，冗余电源。**(实质性要求，提供相应承诺函)**

2）探针应具备:全流量采集、流量识别还原、攻击检测、加密流量检测、敏感信息识别、威胁情报等功能。

3）全流量采集:通过探针实现四川省生态环境厅网络的核心节点流量的采集，支持对IPv4和IPv6网络流量采集。

4）流量识别还原:支持常见协议、数据库协议、文件传输协议识别并还原网络流量，同时支持对隧道封装的流量进行识别还原。

5）攻击检测:支持对WEB攻击、WEBSHELL攻击、暴击破解攻击、挖矿攻击、混淆攻击、反序列化攻击、提权攻击、远程执行攻击等行为的检测。

6）加密流量检测:支持隐秘信道检测。检测类型包括：ICMP、DNS协议等隐蔽隧道攻击检测，恶意软件加密通信的检测，加密web应用的流量检测，非法应用加密通信的检测，SSL加密协议相关的漏洞与攻击的检测，加密通道攻击行为检测，支持指纹检测。

7）敏感信息识别:支持判断告警详情是否包含身份证号、用户名、密码等敏感信息，并对敏感信息脱敏展示。

8）威胁情报：探针本地集成威胁情报数据，威胁情报总量不低于800万，支持统计展示威胁情报检测命中数。

4.终端安全运维服务

为保证终端的安全性，实现终端数据的安全管控，投标人在服务期间需提供500台的终端(含windows终端、信创终端、服务器)防护软件安全服务。通过控制中心进行统一管理，建立统一的终端安全防御体系，实现对四川省生态环境厅办公用户终端的防病毒、补丁修复、安全管控、垃圾清理、启动项管理等功能。且该软件性能和功能需满足以下参数要求。

（1）标准机架设备，软硬件一体平台，控制中心配置内存16G，存储4T，需提供1套管控中心及用户端防护软件安全服务，具备策略下发、全网终端健康状况监测、防病毒、补丁管理、主机防火墙、终端管控等功能以及服务期内特征库升级服务。

（2）客户端兼容:软件客户端具有良好的兼容性，可安装在Windows XP_SP3及以上/Windows 7/Windows 8/Windows 10/windows 11、中标麒麟、银河麒麟、麒麟V10、统信UOS v20、CentOS 5-8/Red Hat Enterprise Linux 5-8/Ubuntu1610等操作系统上。

（3）支持页面展示在线终端数量、风险终端数量及占比、风险告警数、控制中心当前CPU、内存、硬盘使用百分比、终端在线率、终端正常率、终端操作系统统计、病毒查杀趋势、感染病毒终端、漏洞补丁统计等信息。

（4）客户端主程序、病毒库版本支持按分组和多批次进行分阶段更新，保持在低风险中完成终端能力更新。

（5）支持终端密码保护功能，支持终端“防退出”密码保护、“防卸载”密码保护，可有效防止客户端进程被恶意终止、注入、提高客户端进程、数据、配置的安全性。**（提供第三方机构出具的具备CMA标识的检测报告证明材料）**

（6）支持终端资产登记功能，支持登记终端资产信息以及与资产使用人绑定，资产使用人可以自主绑定资产，同时可设置开机提醒，终端开机后弹出资产登记消息弹窗。

（7）支持病毒防护策略设置，能够设置病毒扫描文件夹范围、是否扫描压缩包、扫描的压缩包层数、扫描时对电脑资源占用的限制、病毒处理方式等。

（8）支持终端主动防御，包括进程防护、驱动防护、入口防护、系统账号防护、远程登录防护、勒索软件防护、挖矿软件防护等。**（提供第三方机构出具的具备CMA标识的检测报告证明材料）**

（9）支持终端漏洞发现识别与补丁管理功能，支持对国产操作系统、Windows操作系统的漏洞进行发现识别，并针对性的打补丁修复。可支持热补丁漏洞修复，降低风险暴露。

（10）支持设置终端访问控制规则，进行场景访问控制操作，支持TCP协议、UDP协议、TCP+UDP协议、ICMP协议、多播和组播、任意协议等类型的规则，支持对IPv4和IPv6地址进行访问控制。

（11）支持外设管控功能，支持禁用USB接口设备、USB移动存储设备、U盘读写、手机盘符、光驱、打印机、扫描仪、摄像头、手机、平板等设备。

（12）支持违规外联检测功能，支持对互联网出口地址探测，支持对违规的互联网出口进行发现、断开网络、终端锁屏、断网+锁屏处理。

5.信息安全设施基础保障服务

（1）安全设备特征库升级授权服务

四川省生态环境厅已购买的防火墙、流量控制系统、终端威胁防御系统的特征库升级授权即将到期，为保障生态环境厅网络的安全防御能力，确保网络安全防护体系的稳定、可靠、安全、高效、流畅运行，本次项目需采购以下设备一年特征库升级授权。

序号	设备类型	设备品牌	数量	型号	特征库类型

1	防火墙	华三	4	SecPath F1000-AI-65（2台）	UFLT特征库升级、AV特征库升级、IPS特征库升级
				SecPath F5000-AI-15（2台）	AV特征库升级、AVG特征库升级、IPS特征库升级
2	防火墙	启明星辰	4	USG-FW-4000-T-NF3210(2台)、USG-FW-4000-T-NF3220（2台）	入侵防护特征库升级、病毒防护特征库升级、应用特征库升级、URL分类特征库升级
3	防火墙	迪普	2	FW1000-GM-A	AV特征库升级、IPS特征库升级
4	入侵防御系统	迪普	2	IPS2000-GC-XI	防病毒特征库、URL特征库、入侵防御特征库
5	流量控制系统	北京派网	2	PB-1230	应用特征库升级服务

（2）入侵防御系统使用服务

为提升生态环境厅网络稳定性和安全防护能力，降低网络链路单点故障，风险供应商在服务期间提供2台入侵防御系统使用服务。设备性能和功能需满足以下参数要求：

★1）标准机架式设备，冗余电源，4T硬盘，千兆光口≥4个，具备BYPASS功能的10/100/1000Base-T接口≥4个，万兆光口≥4个，扩展插槽≥2个。**(实质性要求，提供相应承诺函)**

★2）设备最大并发连接数≥800万，每秒新建HTTP连接数≥20万，网络层最大吞吐量≥40G，IPS吞吐量≥6G。**(实质性要求，提供相应承诺函)**

3）支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、Frag Flood、DNS Flood、HTTP Flood、NTP Query Flood 、NTP Reply Flood和SIP Flood 攻击等。

4）支持基于安全区域的异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、IP选项、TCP异常、Smurf、Fraggle、Land、Winnuke、DNS异常、IP分片、拒绝服务攻击、NTP monlist等。

5）支持漏洞利用攻击防护，包括“永恒之蓝”、“震网三代”、“Struts”、“Struts2”、“Xshell 后门代码”等的漏洞利用攻击防护,针对该类攻击可设置阻断、重置、日志记录等动作。

6）支持暴力破解攻击防护，至少支持文件传输 FTP、邮件传输 IMAP、远程控制台 VNC、远程登录 Telnet、远程桌面 RDP 等协议的暴力破解防护。

7）支持自定义漏洞特征，包括可自定义漏洞的源/目端口、CVE 编号、CNNVD 编号等内容，以保证自定义漏洞的准确性。

（3）数字水印系统使用服务

随着四川省生态环境厅信息化建设的深入推进,核心业务系统承载了大量业务数据，然而，在日常办公场景中，存在通过屏幕拍照、截屏、录屏等方式导致信息外泄的风险隐患，现拟采购一套屏幕水印防泄漏系统，通过以 API 接口的方式，为现有业务系统关键页面提供水印能力调用支持，通过标准化接口与业务系统对接，实现水印策略的灵活配置与动态加载，确保系统关键页面内容叠加高强度可追溯水印信息，提升内部信息安全管理水平。

1）提供网页水印服务应用管理功能，能够对需要添加水印的应用系统进行添加、删除等管理。

2）提供网页水印配置服务，可以根据需求配置水印内容，包括字体、颜色、透明度、用户名、实时时间等，同时支持在线预览，可以查看水印效果是否符合需求。

3）提供网页水印任务管理服务，配置水印任务，提供水印任务管理，任务启动/停止，对业务系统的水印服务进行控制。

4）提供网页水印溯源服务，支持通过网页水印的信息进行溯源。

5）提供网页水印展示、网页打印监视、网页复制监视服务。

6）提供网页水印日志审计，查询水印使用统计，分类汇总，审计服务。

6.项目管理要求

（1）供应商应具有与本项目匹配的服务能力。

（2）项目人员要求

在项目实施或服务过程中，按照采购人需求和岗位要求，需明确 1 名项目经理负总责，项目经理应具有丰富的网络安全服务项目管理、咨询、沟通协调能力，具有预见和应对项目风险能力，对项目实施质量总体把控。除此之外，网络安全基础运维保障服务至少包括 5 名安全技术支持服务人员（包含 2 名驻场人员，其中一名安全专家）提供远程或现场支持，遇重大节假日或检查演练任务根据采购人要求需到现场值守。

实施队伍的人员数量和专业水平应严格符合招标文件相关要求。本项目的驻

场人员应接受采购人的考勤管理并自始至终专职承担本项目工作。未经采购人批准，不得随意更换项目经理和（或）团队成员。因离职、疾病、意外事故等供应商无法控制的原因更换的，需提前和采购人沟通，并提供同等及其以上资质的人员供采购人考察。

根据项目实施情况，采购人有权要求供应商更换团队人员，供应商应在采购人提出更换团队人员后5个工作日内予以更换。更换的人员资质证书不得低于现有人员的资质证书。

（3）项目实施要求

供应商在服务期内应提供7*24小时技术支持服务，服务方式包含但不限于现场、语音电话。服务请求应在10分钟内响应，如现场人员解决不了，高级技术人员应于1个小时内到达现场，应于2小时内处理相关故障，并形成书面处理记录。在服务过程中，根据采购人要求，供应商有义务对采购人相关人员进行相关安全技术培训。

供应商对过程数据和结果数据严格保密，未经采购人授权不得公开发布、泄露给任何单位和个人，不得利用此数据进行任何侵害采购人的行为，否则采购人有权追究供应商的责任。供应商提供的技术服务，不得侵犯任何第三方的合法权益，由此而引起的纠纷或者给第三方以及采购人造成的损失，应由供应商承担全部责任。

供应商服务过程中发现危害或可能危害国家安全、公共利益的网络安全风险事件，应及时报告。涉及安全漏洞的，不得擅自出售、透露、转让、公布漏洞的技术细节、利用方法、工具等。供应商不得向服务范围内涉及的单位额外或变相收取费用，或者要求其购买指定产品或服务。

（4）协助设备安装调试要求

供应商应派遣技术小组到现场协助采购人实施设备安装、软硬件的测试和调整服务、设备更新、现场培训等服务。设备安装、调试的主要目标是使整个系统能够正常运行，确保与之相连的全部设备正常连通。供应商需按照采购人要求，根据项目需求完成现有网络及安全等设施的集成、调试工作。

（5）服务保障要求

服务期正式计算后，供应商需提供技术支持和服务，服务内容应包括但不限于下述内容：升级服务、定期巡检、性能调优、应急响应、分析报告、协助采购人故障排除和故障排除所需的备件更换（含备件本身）、产品的安装部署上线、与其他系统的集成等。服务方式应包括电话支持、电子邮件支持、文档提供、现场支持等多种以解决实际问题为目的的方式。

（6）项目配合要求

协助、配合采购人、监理单位和测评单位的工作，按照经采购人同意的技术要求和实施计划要求进行项目实施，完成与项目有关的采购人提出的其他任务，并配合相关集成工作，完成与本项目有关的采购人提出的其他任务。设备应提供第三方接口，满足统一管理的要求。供应商项目实施、人员等管理按照采购人项目管理制度执行。

供应商在项目实施过程中应遵循国际、国内相关标准及技术规范要求进行实施，提供要素齐全的成果报告资料，并对其负责。交付物包含但不限于服务要求的所有报告。

★7.信息化系统运维维护服务的违约和罚则（实质性要求,提供相应承诺函）

1.供应商在政府采购过程中提供的所有文件须真实可靠，中标后四川省环境信息中心将检查供应商在政府采购过程中提供的以及投标文件中提供的所有材料的原件、复印件以及供应商工作场所，并视情况考察供应商提供的所有项目案例。

供应商应当按照四川省环境信息中心相关检查要求以及投标时的各项承诺，配合四川省环境信息中心开展各项检查工作，确保各项检查工作的正常进行。

2.在政府采购和招标工作的任何阶段发现供应商有任何欺骗行为，投标文件有虚假内容或不实承诺的，采购人将上报财政监管部门，由供应商自行承担一切损失，并依法追究供应商法律责任。

3.如遇供应商不能按照招标文件中的时间要求完成故障处理，四川省环境信息中心有权邀请第三方公司提供相关紧急故障恢复和备品备件或备机服务，由此发生的所有费用由供应商承担。

4.在履约期间出现被公安、网信、生态环境部等主管部门通报的情形，每次扣收0.5%的合同金额。

5.考核规则

运维期结束前一个运维季度内，采购人对服务方进行运维绩效考评，考评时，按照合同要求的服务内容，对照运维质量考评表中“考评要求”逐项进行考评，特殊 事项填写“备注”说明，评分表可以根据后续工作实际情况进行调整。

考评分值达到 80 分以上，采购人即可按照最终验收时间向中标方无息退还履约保证金。 若考评分值未达 80 分，按照以下标准扣收合同金额：

（1）考评分值71～80分的，扣收5%的合同金额。

（2）考评分值60～70分的，扣收10%的合同金额。

（3）考评分值60分以下的，终止项目合同，算供应商单方面违约。

服务绩效考评表

序号	考评类别	考评要求	计分标准	得分	备注

1	服务响应（10分）	提供7×24小时的故障申报热线服务，响应时间为30分钟	未及时响应、协调并处置故障，影响系统正常使用的，每次扣2分，扣完为止。		
2	故障处理服务（25分）	系统、设备运行过程中如果发生故障，对故障的恢复时间不超过30分钟（10分）	未在规定时限内积极联系厂商解决故障，影响系统、设备正常使用，每次扣2分，扣完为止。		
		系统、设备运行过程中系统、设备接口如果发生故障，对故障的恢复时间不超过1小时(10分）	未在规定时限内积极联系厂商解决故障，影响系统、设备正常使用，每次扣2分，扣完为止。		
		年故障时间应该小于24小时，总故障数应该小于10次(5分）	优秀：年故障时间<24小时，总故障数＜10次，得5分。		
			一般：24小时≤年故障时间<36小时，10次≤总故障数≤15次，得2～4分。		
			较差：36小时≤年故障时间，15次＜总故障数，得0～1分。		
3	应急保障服务（10分）	各种紧急情况配备相应资源，按用户要求提供现场或者远程的7×24小时技术支撑服务，确保系统正常运行。响应时间为30分钟	未及时做出应急响应服务，每次扣2分，扣完为止。		
4	省厅驻场服务工作质量（20分）	是否及时完成运维事项和交办任务，并保证完成质量	优秀：能够按时完成运维工作事项和交办任务，质量较好，得16～20分。		
			合格：能够按时完成运维工作事项和交办任务，质量合格，得10～15分。		
			一般：基本能够完成运维工作事项和交办任务，质量一般，得5～9分。		
			较差：不能按要求完成运维工作事项和交办任务，低级错误频发，得0～4分。		
5	过程文档（5分）	服务过程中产生文档及各时间节点的总结报告提交的完整性、及时性。	未按时或未完整提交每次扣1分，扣完为止。		
6	其他（30分）	网络安全隐患排查情况(15分）	被省委网信办、省公安厅、生态环境部等主管部门检查出网络安全隐患，一处隐患扣5分，扣完为止。		

			被第三方安全公司检测出网络安全风险，且网络安全风险被采购人认定为中标方运维服务中本应该检测出来的问题，一次扣 2.5 分，扣完为止。		
		攻防演练情况（15 分）	省级以上攻防演练中，因省厅被破防造成生态环境部失分，扣 10 分。		
			省级攻防演练被攻破出局，扣 15 分。		
			省级攻防演练失分，扣 10 分。		
			防守良好，得 15 分。		

五、★其他要求（实质性要求，提供相应承诺函）

1.供应商须提供书面承诺函（格式自拟），承诺对服务期间所提供的所有软硬件设备提供原厂技术支持、授权升级服务。

2.供应商须提供书面承诺函（格式自拟）：在服务期间，供应商提供服务中使用的安全产品若在《网络关键设备和网络安全专业产品目录》内，则该安全产品须具备有效期内的《计算机信息系统安全专用产品销售许可证》(备注：限 2023 年 7 月 1 日前已经获得销售许可证的产品且在有效期内的提供)或已列入国家网信办公开发布的《网络关键设备和网络安全专用产品安全认证和检测结果》中。