四川省生态环境保护信息安全体系项目技术方案

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

2021 年我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 2024 年 10 月到期。今年，在四川省生态环境厅现有信息安全体系基础上，继续采购网络和信息安全保障服务，包括日常运维、应急响应、人员驻场等服务，在日益严格的安全监管要求和日益严峻的网络安全形势下，能全方位保障我厅网络和信息安全，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 2024 年 10 月 31 日至 2025 年 5 月 31 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。

1.1 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。

1.2 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。

1.3 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，本次项目需按照甲方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，其中包含驻场人员且驻场人员必须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（根据甲方实际需求变化进行调整）进行维护，包含巡检、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、密码维护、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
1	一级防火墙 01（主）	1
2	一级防火墙 02（备）	1
3	二级防火墙 01	1
4	二级防火墙 02	1
5	上联防火墙 01	1
6	上联防火墙 02	1
7	电子政务外网防火墙 01	1
8	电子政务外网防火墙 02	1
9	互联网入侵防御系统 01	1
10	互联网入侵防御系统 02	1
11	下联防火墙 01	1
12	下联防火墙 02	1

13	专网入侵防御系统	1
14	堡垒机	1
15	抗 DDOS	2

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。协助甲方进行网络链路维护、优化、改造及拓扑图整理。

4）网络故障排查。协助甲方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、网络安全审计等安全设施，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。按照甲方需求，对四川省生态环境厅业务系统开展安全风险隐患排查，进行漏洞扫描、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，督促跟踪汇总修复情况。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。为甲方提供网络安全体系、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，协助甲方建立关键信息基础设施保护体系等。

9）目前省厅业务系统已迁移至政务云，协助甲方对云服务商提供的安全能力进行监督检查，对云服务商日常安全运维工作（安全应急演练、漏洞扫描、渗透测试、日常安全策略开通、配置备份、重大保障、培训等）进行督促、检查、指导，督促云服务商做好政务云业务系统的日常安全管理和防护工作，保障业务系统安全稳定运行。

1.4 驻场服务

★按照采购人工作需求和人员要求，提供驻场服务，驻场服务期间长期驻场人员不低于 3 人，其中安全专家 1 名。

驻场人员需完成甲方安排的工作，并纳入甲方内部管理制度统一管理，服从

采购人值班安排（含夜班和节假日值班值守，值班费由供应商承担）。

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，和甲方能够进行顺畅有效沟通，能及时理解甲方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。

2.1 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

2.2 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。

2.3 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），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。

在国家、部、省组织的安全演练活动中，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。

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，供应商应针对本项目安全服务提供统一态势感知安全平台服务，包括：

3.1 态势感知系统

通过态势感知平台实现全网海量数据规模的安全信息的采集和集中存储，实现各类型多厂商安全监测防护资源的整合，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。

安全监测：通过平台实现对四川省生态环境厅网络安全事件的集中监测，实时查看安全状态信息和事件记录，监控整体网络的安全风险和运行环境的变化，确保安全防护措施处于正常运行状态。对在安全运营中监测到异常情况及时进行安全告警。

1）支持对监测设备的集中管理；

2）支持对监测设备监测到的内容进行管理；

3）实现对安全事件、全网安全状态和监测设备运行状态进行实时监控和告警。

4）支持监测的设备包括但不限于防火墙、IPS、路由器、交换机、服务器等。

可视化态势呈现：通过对收集的数据进行深度分析，集中全部获取的安全信息进行综合安全态势呈现，将复杂的网络安全数据以直观的图表、地图等形式展现，从全局的角度把控四川省生态环境厅全网安全状态，有助于及时有效的应对网络攻击。可视化态势呈现是网络安全防御体系中的重要组成部分，它不仅提高了监测和响应能力，还能够有效地管理和优化整个网络安全防御流程。

1）支持通过地图的方式展示来自各地区的攻击情况；

2）支持对当前省厅全网资产安全态势进行分析呈现；

3）支持展示全网漏洞情况以及业务系统的健康情况。

3.2 态势感知探针

网络安全态势感知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。供应商需提供 2 台态势感知探针，通过探针制定规则采集网络信息数据，包括网络会话信息、HTTP 访问信息、FTP 传输样本文件信息、DNS 信息、网络攻击事件信息等，通过 Syslog、SNMP Trap 方式实现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）探针应具备：全流量采集、入侵检测、病毒检测、未知威胁行为检测、僵木蠕检测、实时监控等功能。

2）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，并按自定义格式文件方式存储采集的网络数据。

3）入侵检测：对网络流量进行深度包解析和流解析，实现病毒、木马、蠕虫、僵尸网络、缓冲区溢出攻击、拒绝服务攻击、扫描探测、欺骗劫持、SQL 注入、XSS 攻击、网站挂马、隐蔽信道、AET 逃逸、C&C 行为等各种威胁的全面有效检测。

4）病毒检测：通过特征匹配或检测算法对被检测文件的文件内容进行检测，以此来确定文件是否为恶意文件。

5）未知威胁行为检测：对未知木马 C&C 行为、网络扫描行为、蠕虫行为进行检测，发现未知威胁行为。

6）僵木蠕检测：通过僵木蠕事件库，发现在网络中存在已经被种植上木马或者已经被外部的黑客控制的终端或者是设备，定位到危险源头。

7）实时监控：对流量、互联关系进行实时监控，流量监控包括端口、服务、IP 等。

4.终端运维服务

四川省生态环境厅已购买的终端防护软件授权即将到期,病毒防护功能即将失效。为保证终端的安全性，实现终端数据的安全管控，供应商需在服务期间需提供 600 台的终端防护软件安全服务（终端防护软件需甲方确认后用于服务）。通过控制中心进行统一管理，建立统一的内网安全防御体系，实现对四川省生态环境厅办公用户终端和业务应用物理服务器的防病毒、补丁修复、安全管控等功能。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≧10G,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。包含防病毒、补丁管理、运维管控、数据日志审计、授权许可模块、服务期内特征库服务升级。

2)资产采集：支持网络资产自动发现、采集、并按照相应规则进行设备分类。主要采集信息包括计算机名称、IP 地址、漏洞数、病毒数、病毒库更新时间、

安全防护开启状态等。

3)资产统计：可以支持按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息，可监控CPU温度、硬盘温度和主板温度。

4)特征库升级：支持特征库定期自动更新升级，支持手动更新控制中心更新包，支持本地升级病毒库。具备定时漏洞修复功能，同时可以支持设置筛选高危漏洞、软件更新、功能性补丁等修复类型进行选择性修复。

5)终端防护软件需支持windows、LinuX操作系统和常见的国产化操作系统（包括中标麒麟、银河麒麟、统信USO等）。

6)补丁管理：对全网计算机、服务器进行漏洞扫描、补丁修复、在保障网络带宽的前提下可以有效提升整体漏洞防护等级,终端防护软件需具备漏洞集中修复、强制修复、自动修复、选择性修复功能，支持热补丁功能和系统修复功能，支持补丁回退功能，强制卸载已安装的补丁，支持使用离线补丁下载补丁及导入补丁到服务器。

7)漏洞修复支持漏洞利用防御,尤其对通过文件漏洞的攻击行为进行有效检测与防御。

8)病毒防护：终端防护软件需支持平台集中病毒查杀功能，支持闪电查杀、全盘查杀、自定义文件查杀功能，支持自定义通过快速查杀、全盘查杀、自定义查杀文件夹任务发现病毒后进行自动清除。支持对宏病毒、蠕虫病毒、勒索病毒、木马程序、恶意软件等已知或未知病毒的查杀。

9)审计功能：终端防护软件需能够对安装软件的终端进行基本的行为审计，包括外接设备的使用、软件使用、文件操作、设备开机、系统账户登录等进行一定的日志纪录。

10)准入控制功能：终端防护软件需具备准入控制功能（未安装终端防护软件，则无法接入指定单位网络）。支持对终端进行准入控制，对入网终端进行身份认证，包括对IP地址、MAC地址、基于用户名和密码的身份的管理。

11)策略管理：终端防护软件需支持终端密码保护，启用密码保护功能后，终端退出或卸载客户端，都需要输入正确的密码方可执行。支持自定义策略生效时间，在不同的时间段执行不同的策略，包含工作时间和非工作时间两种模式。支持对终端本地的安全策略使用权限进行配置。支持对终端密码进行加固，实现

密码复杂性要求、密码长度和密码最短使用期限，支持基于字典的弱密码检测等功能。

12)设备管理：终端防护软件需支持根据设备类型对终端外设的使用权限进行管控，启用或禁用，支持对外设设备的统计，支持自动收集终端曾经使用过的USB设备的历史记录并上报服务器，可对指定范围终端的USB设备使用历史进行查询。

13)软件分发：终端防护软件需支持客户端软件安装包的自动分发和安装，管理控制台可以对指定台式机或服务器（或群组）推送软件，同时，被推送的软件在到达终端之后，可以选择是否立即安装。且支持MSI、EXE、BAT、脚本等格式的安装程序，支持自定义安装包，支持普通格式文件自动分发，可以将文件自动分发到指定的终端目录下，支持记录、统计和查询客户端软件分发完成情况。

14)终端防护软件支持发生违规外联时可对内外网链接状态分别设置违规处理措施。

5.项目管理要求

5.1 项目实施要求

在项目实施或服务过程中，供应商应组织一支技术水平高、业务能力强、服务态度好的实施队伍。按照采购人需求和岗位要求，实施队伍至少包括5名安全技术支持服务人员提供远程或现场支持，其中明确1名项目经理负总责，长期驻场人员不低于3人，遇重大节假日或检查演练任务需到现场值守。

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招标人的考勤管理并自始至终专职承担本项目工作。未经招标人批准，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招标人考察。

根据项目实施情况，招标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。

5.2 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、调测的主要目标是使整个系统能够正常运行，确保与之相联的全部设备正常联通。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。

5.3 服务保障要求

服务期间，如平台发生故障，须在 2 小时内对采购人所提出的维修要求做出实质性反应并及时解决，恢复时间不能超过 24 小时，故障恢复期间应确保系统不中断。平台服务期限内，平台发生的一切故障维修费用由供应商承担。

服务期正式计算后，供应商须提供免费的技术支持和服务，免费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。服务的所有报价都需要计入中标总价中，否则视为免费。

5.4 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，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。

6.信息化系统运维维护服务的违约和罚则

（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，四川省环境信息中心有权中止合同并进行索赔，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）考核规则

每年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函。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分及以下的，终止项目合同，算乙方单方面违约。

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	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。 10分		
		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	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。 10分		
		年故障时间应该小于24小时，总故障数应该小于10次	优秀:年故障时间<24小时，总故障数＜10次。 5分		
			一般：24小时<年故障时间<36小时，10次≤总故障数≤15次。		

			2-4 分		
			较差:36 小时<年故障时间，15 次<总故障数。 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。		
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 （20 分）	优秀：能够按时完成运维工作事项和交办任务，质量较好。 （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。（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。（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。(1-4 分)		
5	过程文档 （5 分）	运维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。	对于故障处理，2 日内提供故障说明文档；定期巡检，一月一次，每月 10 号前提供上一月的巡检报告；运维期满一年后，一周内提供年度运维总结报告。未按时或未完整提交每次扣 1 分。		
6	其他 (30 分)	网络安全隐患排查情况（10 分）	被省委网信办、省公安厅、生态环境部等检查出网络安全隐患，一处隐患扣 2 分，扣完为止。 6 分		
			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 1 分，扣完为止。 4 分		
		攻防演练情况	省级以上攻防演练中，因省		

		（20 分）	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 20 分。		
			防守良好，得 20 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），承诺驻场服务期间长期驻场人员不低于 3 人，其中安全专家 1 名。

3. 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，则该安全产品需具备有效期内的《计算机信息系统安全专用产品销售许可证》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。